Cloud Service Engine

User Guide

Issue 01

Date 2024-10-15

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

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

1 Before You Start

Cloud Service Engine (CSE) is a cloud middleware used for microservice applications. It supports ServiceComb engines contributed to Apache and open-source enhanced Nacos engines. You can also use other cloud services to quickly build a cloud-native microservice system, implementing quick development and high-availability O&M of microservice applications.

Prerequisites

1. You have **registered a Huawei Cloud account and enabled Huawei Cloud services**.
2. The login account has the permission to create a microservice engine. For details, see **Creating a User and Granting Permissions**.

Logging In to the CSE 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 select **Cloud Service Engine** in the service list. The CSE console is displayed.

NOTE

- You are using CSE instances provisioned from ServiceStage. If you want to provision new instances from CSE, please grant permissions to CSE.
- CSE needs the Virtual Private Cloud (VPC) and Domain Name Service (DNS) services to run. If you have not granted any permissions, create a cloud service agency to grant permissions to CSE.

Once a service has been authorized, an agency named cse_admin_trust on IAM will be created. Go to the agency list to view the details. To grant permissions, you must have the Security Administrator role permissions. Confirm the permissions in the IAM service.

Without permissions, some CSE functions will be affected, including engine creation and upgrade and security authentication enabling/disabling.

----End

2 Permissions Management

2.1 Creating a User and Granting Permissions

This section describes how to use **IAM** to implement fine-grained permissions control for your CSE resources. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials for access to CSE resources.
- Grant only the permissions required for users to perform a task.
- Entrust a Huawei Cloud account or cloud service to perform professional and efficient O&M on your CSE resources.

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

This section describes the procedure for granting permissions (see **Figure 2-1**).

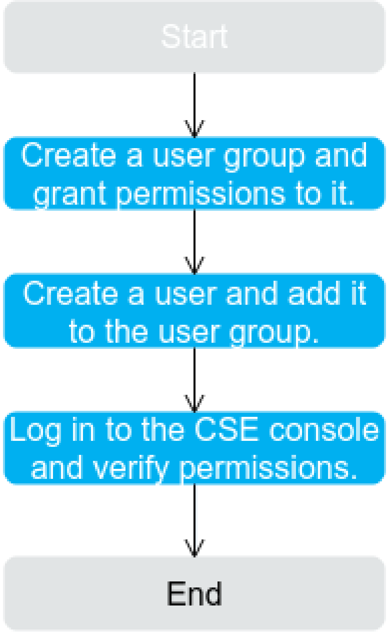
Prerequisites

Before assigning permissions to user groups, you should learn about CSE policies and select the policies based on service requirements.

- For details about system permissions supported by CSE, see **Permissions Management**.
- For details about the permissions of other services, see **System Permissions**.

Process Flow

Figure 2-1 Process of granting CSE permissions


Start
Create a user group and grant permissions to it.
Create a user and add it to the user group.
Log in to the CSE console and verify permissions.
End

1. Create a user group and grant permissions to it.

   Create a user group on the IAM console, and grant the **CSE ReadOnlyAccess** policy to the group.

2. Create a user and add it to the user group.

   Create a user on the IAM console and add the user to the group created in **1**.

3. Log in to CSE and verify permissions.

   Log in to the CSE console as the created user, and verify that it has the read-only permission for CSE.

   - In **Service List**, choose **Cloud Service Engine**. On the console, choose **ServiceComb** > **Buy Exclusive Microservice Engine**. If a message is displayed indicating insufficient permissions, the **ReadOnlyAccess** policy has taken effect.
   - Choose any other service in **Service List**. If a message is displayed indicating insufficient permissions to access the service, the **ReadOnlyAccess** policy has taken effect.

2.2 Creating a Custom Policy for a Microservice Engine

Custom policies can be created as a supplement to the system policies of CSE.

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 policy in the JSON format from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. The following section contains examples of common CSE custom policies.

Example Custom Policy

This procedure creates a policy that an IAM user is prohibited to create and delete a microservice engine.

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Action": [
                                "cse:*:*"
                        ],
                        "Effect": "Allow"
                },
                {
                        "Action": [
                                "cse:engine:create",
                                "cse:engine:delete"
                        ],
                        "Effect": "Deny"
                }
        ]
}
```

A deny policy must be used in conjunction with other policies to take effect. If the permissions assigned 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 verify that a user is not allowed to create microservice engines on the console.

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. Create a microservice engine on the CSE console. If error 403 is returned, the permissions are correct and have taken effect.

3 Exclusive ServiceComb Engine

3.1 Creating a ServiceComb Engine

This section describes how to create a ServiceComb engine.

NOTE

ServiceComb engines are supported only in CN East 2, CN-Hong Kong, ME-Riyadh, TR-Istanbul, AP-Singapore, and AP-Jakarta.

Prerequisites

A ServiceComb engine runs on a VPC. Before creating a ServiceComb engine, ensure that a VPC and subnet are available.

You have created a VPC. For details, see **Creating a VPC**.

If the engine is created using an account with the minimum permission for creating engines, for example, **cse:engine:create** in the **fine-grained permission dependencies of microservice engines**, the default VPC security group cse-engine-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 cse-engine-default-sg rules

Direction	Priority	Policy	Protocol and Port	Type	Source Address
Inbound	1	Allow	ICMP: all	IPv6	::/0
	1	Allow	TCP: 30100–30130	IPv6	::/0
	1	Allow	All	IPv6	cse-engine-default-sg

Direction	Priority	Policy	Protocol and Port	Type	Source Address
	1	Allow	TCP: 30100–30130	IPv4	0.0.0.0/0
	1	Allow	ICMP: all	IPv4	0.0.0.0/0
Outbound	100	Allow	All	IPv4	0.0.0.0/0
	100	Allow	All	IPv6	::/0

Creating a ServiceComb Engine

Step 1 Go to the **Buy Exclusive ServiceComb Engine** page.

NOTE

- By default, a maximum of five exclusive ServiceComb engines can be created for each project. To create more, submit a service ticket to increase the quota. For details, see **Creating a Service Ticket**.
- For details about projects, see **Projects**.

Step 2 Set parameters according to the following table. Parameters marked with an asterisk (*) are mandatory.

Parameter	Description
*Billing Mode	Billing mode. Currently, **Pay-per-use** is supported.
*Enterprise Project	Select the project where the ServiceComb engine is located. You can search for and select the required enterprise project from the drop-down list. Enterprise projects let you manage cloud resources and users by project. An enterprise project can be used after it is created and enabled. For details, see **Enabling the Enterprise Project Function**. By default, **default** is selected. **NOTE** When a ServiceComb engine is in use, do not disable the enterprise project. Otherwise, the engine will not be displayed in the engine list, affecting normal use.
*Instances	Select the microservice instance quota.
*Engine Type	ServiceComb engine type. If the engine type is cluster, the engine is deployed in cluster mode and supports host-level DR.

Parameter	Description
*Name	Name of a ServiceComb engine. The name contains 3 to 64 characters, including letters, digits, and hyphens (-), and starts with a letter but cannot end with a hyphen. **NOTICE** ServiceComb engine name cannot be **default**.
*AZ	Availability zone. Select one or three AZs for the engine based on the number of AZs in the environment. ● Select one AZ to provide host-level DR. ● Select three AZs to provide AZ-level DR. **NOTE** ● The AZ of a created ServiceComb engine cannot be changed. ● The AZs in one region can communicate with each other over an intranet. ● Multiple AZs enhance DR capabilities.
*Network	Select a VPC and subnet to provision logically isolated, configurable, and manageable virtual networks for your engine. ● To use a created VPC, search for and select a VPC created under the current account from the drop-down list. ● To use a new VPC, click **Create VPC** in the drop-down list. For details, see **Creating a VPC**. ● To use a shared VPC, select a VPC that another account shares with the current account from the drop-down list. VPC owners can share the subnets in a VPC with one or multiple accounts through **Resource Access Manager (RAM)**. Through VPC sharing, you can easily configure, operate, and manage multiple accounts' resources at low costs. For more information about VPC and subnet sharing, see **VPC Sharing**. **NOTE** The VPC cannot be changed once the engine is created.
Description	Click ✎ and enter the engine description.
Tag	Tags are used to identify cloud resources. When you have multiple cloud resources of the same type, you can use tags to classify them based on usage, owner, or environment. Click ⊕ **Add Tag**. In the **Add Tag** dialog box, enter a tag key and value. For details about tag naming rules, see **Managing Tags**. In the **Add Tag** dialog box, you can click ⊕ **Add Tag** to add multiple tags at a time, or click ⊖ next to a tag to delete the tag.

Parameter	Description
Authentication Mode	The exclusive ServiceComb engine with security authentication enabled provides the system management function using the role-based access control (RBAC) through the microservice engine console. ● Select **Enable security authentication**: 1. Determine whether to enable **Authenticate Programming Interface**. After it is enabled, you need to add the corresponding account and password to the microservice configuration file. Otherwise, the service cannot be registered with the engine. After it is disabled, you can register the service with the engine without configuring the account and password in the microservice configuration file, which improves the efficiency. You are advised to disable this function when accessing the service in a VPC. 2. Enter and confirm the password of user **root**. Keep the password secure. ● Select **Disable security authentication**: Disable security authentication. You can enable it after the instance is created.

Step 3 Click **Buy**. The page for confirming the engine information is displayed.

Step 4 Click **Submit** and wait until the engine is created.

NOTE

- It takes about 31 minutes to create a ServiceComb engine.
- After the ServiceComb engine is created, its status is **Available**. For details about how to view the ServiceComb engine status, see **Viewing ServiceComb Engine Information**.
- If the ServiceComb engine fails to be created, view the failure cause on the **Operation** page and rectify the fault. Then, you can perform the following operations:
  - In the **ServiceComb Engine Information** area, click **Retry** to create an engine again.
  - If the retry fails, delete the ServiceComb engine that fails to be created. For details, see **Deleting an Exclusive ServiceComb Engine**.

----End

3.2 Managing ServiceComb Engines

3.2.1 Viewing ServiceComb Engine Information

In the **ServiceComb Engine Information** area, you can view the engine information as shown in **Table 3-2**.

Viewing ServiceComb Engine Information

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 In the **ServiceComb Engine Information** area, you can view the engine information as shown in Table 3-2.

Table 3-2 Engine details

Item	Description
Name	Engine name entered when Creating a ServiceComb Engine. Click ⧉ to copy it. Click ✎ to change an engine name. The name contains 3 to 64 characters, including letters, digits, and hyphens (-), and starts with a letter but cannot end with a hyphen.
Engine ID	Engine ID. You can click ⧉ to copy it.
Status	Engine status, which can be: ● Creating ● Available ● Unavailable ● Configuring ● Deleting ● Upgrading ● Resizing ● Creation failed ● Deletion failed ● Upgrade failed ● Resizing failed ● Frozen
Version	Engine version.
Engine Type	Engine type selected when Creating a ServiceComb Engine.
AZ	Availability zone selected when Creating a ServiceComb Engine.
Tag	Tags added to the ServiceComb engine. You can also click **Tag Management** and perform operations on tags as required. For details, see Managing Tags.
Description	Engine description entered when Creating a ServiceComb Engine.

----End

3.2.2 Obtaining the Service Center Address of a ServiceComb Engine

This section describes how to obtain the service center address of a ServiceComb engine. The service center address cannot be changed after the engine is created.

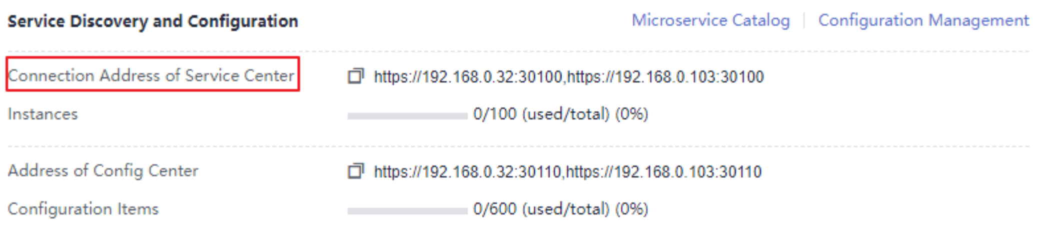
Obtaining the Service Center Address of a ServiceComb Engine

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 In the **Service Discovery and Configuration** area, view the service center address of the microservice engine.



Service Discovery and Configuration

Microservice Catalog | Configuration Management

Connection Address of Service Center	https://192.168.0.32:30100,https://192.168.0.103:30100
Instances	0/100 (used/total) (0%)
Address of Config Center	https://192.168.0.32:30110,https://192.168.0.103:30110
Configuration Items	0/600 (used/total) (0%)

----End

3.2.3 Obtaining the Configuration Center Address of a ServiceComb Engine

This section describes how to obtain the configuration center address of a ServiceComb engine.

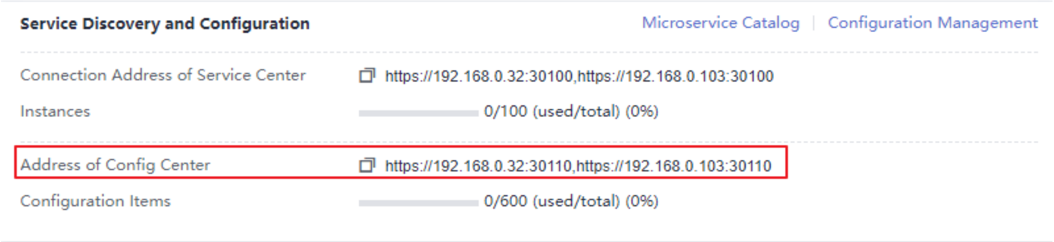
Obtaining the Configuration Center Address of a ServiceComb Engine

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 In the **Service Discovery and Configuration** area, view the configuration center address of the microservice engine.



Service Discovery and Configuration

Microservice Catalog | Configuration Management

Connection Address of Service Center	https://192.168.0.32:30100,https://192.168.0.103:30100
Instances	0/100 (used/total) (0%)
Address of Config Center	https://192.168.0.32:30110,https://192.168.0.103:30110
Configuration Items	0/600 (used/total) (0%)

NOTE

- For ServiceComb engine 1.x, the port number of the configuration center address is 30103.
- For ServiceComb engine 2.x, the port number of the configuration center address is 30110.

----End

3.2.4 Viewing the Instance Quota of a ServiceComb Engine

This section describes how to view the instance quota and quota usage of a ServiceComb engine.

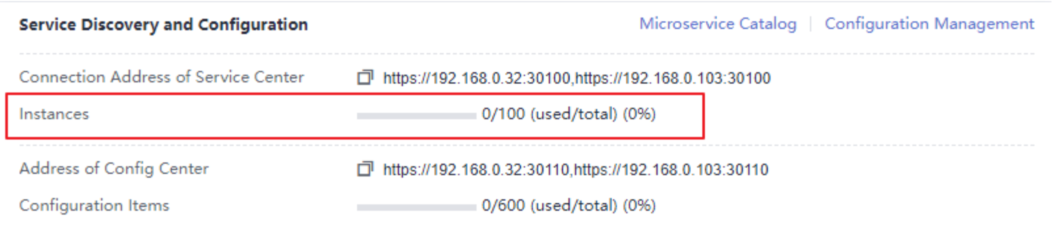
Viewing the Instance Quota of a ServiceComb Engine

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 In the **Service Discovery and Configuration** area, view the instance quota and quota usage of the microservice engine.



Service Discovery and Configuration

Connection Address of Service Center https://192.168.0.32:30100,https://192.168.0.103:30100

Instances 0/100 (used/total) (0%)

Address of Config Center https://192.168.0.32:30110,https://192.168.0.103:30110

Configuration Items 0/600 (used/total) (0%)

----End

3.2.5 Viewing the Configuration Item Quota of a ServiceComb Engine

This section describes how to view the configuration item quota and quota usage of a ServiceComb engine.

NOTE

This section applies only to ServiceComb engine 2.x.

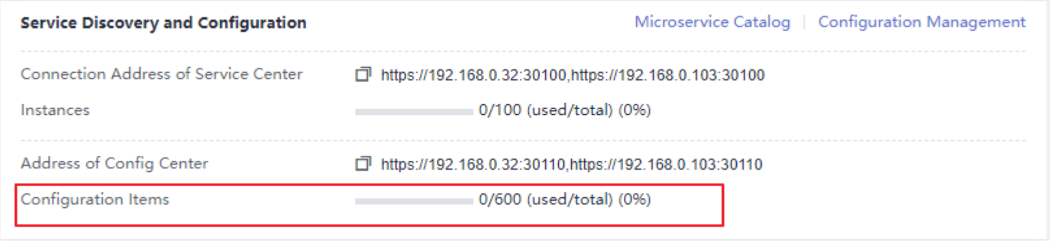
Viewing the Configuration Item Quota of a ServiceComb Engine

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 In the **Service Discovery and Configuration** area, view the configuration item quota and quota usage of the microservice engine.



Service Discovery and Configuration

Connection Address of Service Center https://192.168.0.32:30100,https://192.168.0.103:30100

Instances 0/100 (used/total) (0%)

Address of Config Center https://192.168.0.32:30110,https://192.168.0.103:30110

Configuration Items 0/600 (used/total) (0%)

----End

3.2.6 Configuring Backup and Restoration of a ServiceComb Engine

The microservice console provides the backup and restoration functions. You can back up and restore ServiceComb engine data, including microservices, contracts, configurations, and account roles.

You can customize backup policies to periodically or manually back up ServiceComb engines.

Background

- Each exclusive ServiceComb engine supports a maximum of 15 successful backups, including a maximum of 10 manual backups and a maximum of 5 automatic backups.
- The backup data will be stored for 10 days. Expired backup data will be deleted.

Automatic Backup

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 In the **Backup and Restoration** area, click **Automatic backup settings** and set backup parameters.

Table 3-3 Automatic backup parameters

Parameter	Description
Automatic Backup	After automatic backup is disabled, the previously set backup policy will be deleted. In this case, you need to set the backup policy again.
Backup Interval	Backup period. This parameter takes effect after **Automatic Backup** is enabled.
Trigger Time	Time at which a backup task starts. Only the hour is supported. This parameter takes effect after **Automatic Backup** is enabled.

Step 5 Click **OK**.

Once the backup policy is set, the backup task is triggered within one hour after the preset time.

----End

Manual Backup

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 In the **Backup and Restoration** area, click **Create Manual Backup** and set backup parameters.

Table 3-4 Manual backup parameters

Parameter	Description
Name	Name of a backup task. The name cannot be changed after the backup task is created.
Remarks	(Optional) Description about the backup task.

Step 5 Click **OK**.

----End

Restoring Backup Data

NOTICE

The backup data will overwrite the current data of the ServiceComb engine. As a result, the microservice and service instances may be messed, and dynamic configurations may be lost. Exercise caution when performing this operation.

If security authentication is enabled, the backup data contains the account information. You are advised to disable security authentication before restoring the backup data. Otherwise, the authentication for accessing the ServiceComb engine may fail after the restoration.

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 In the **Backup and Restoration** area, click **Restore** in the **Operation** column of the row that contains the specified backup data.

1. Select **I have read and fully understand the risks**.
2. Click **OK**. To view the restoration status, click **Restoration History** in the **Backup and Restoration** area.

----End

Deleting Backup Data

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 In the **Backup and Restoration** area, click **Delete** in the **Operation** column of the target backup data. In the displayed dialog box, enter **DELETE** and click **OK**.

----End

3.2.7 Managing Public Network Access for a ServiceComb Engine

3.2.7.1 Binding an EIP

Exclusive ServiceComb engines that are bound with EIPs can be accessed from the public network.

NOTICE

ServiceComb engines with security authentication disabled do not have the authentication and authorization capabilities. Opening those engines to the public network may cause security risks and increases the system vulnerability. For example, data assets such as configurations and service information may be stolen.

Do not use this function in a production environment or a network environment with high security requirements.

Prerequisites

An EIP has been created.

For details about how to create an EIP, see **Assigning an EIP**.

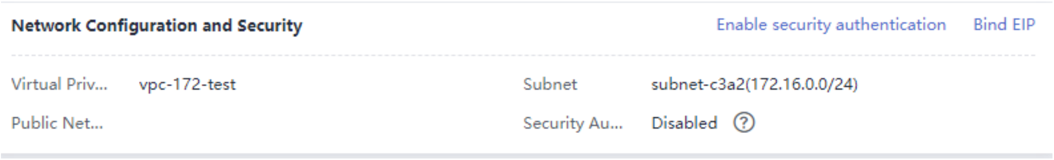
Binding an EIP

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 In the **Network Configuration and Security** area, click **Bind EIP**.



Network Configuration and Security | Enable security authentication | Bind EIP

Virtual Priv...	vpc-172-test	Subnet	subnet-c3a2(172.16.0.0/24)
Public Net...		Security Au...	Disabled ⓘ

Step 5 Read the security risk prompt in the displayed dialog box and select **I understand the security risks**.

Step 6 In the **EIP** drop-down list, select the EIP to be bound.

NOTE

You can only select an EIP in the same enterprise project as the ServiceComb engine.

Step 7 Click **OK**.

----End

3.2.7.2 Unbinding an EIP

If an EIP has been bound to an exclusive ServiceComb engine, you can unbind the EIP from the engine to disable the public network access to the engine.

Unbinding an EIP

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 In the **Network Configuration and Security** area, click **Unbind EIP**.

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

----End

3.2.8 Viewing ServiceComb Engine Operation Logs

In the **Operation** area, you can view the operation logs of a ServiceComb engine.

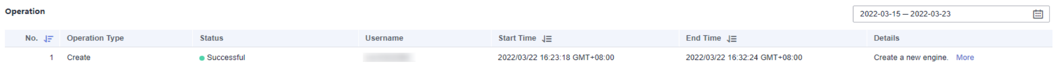
Viewing ServiceComb Engine Operation Logs

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 In the **Operation** area, view the operation logs of a ServiceComb engine.



Operation 2022-03-15 — 2022-03-23

No.	Operation Type	Status	Username	Start Time	End Time	Details
1	Create	● Successful	[redacted]	2022/03/22 16:23:18 GMT+08:00	2022/03/22 16:32:24 GMT+08:00	Create a new engine. More

- Click 📅 in the upper right corner to view operation logs in a specified period.
- Click **More** in the **Details** column of a specified operation log to view details about the operation log.

----End

3.2.9 Upgrading a ServiceComb Engine Version

ServiceComb engines are created using the latest engine version. When a later version is released, you can upgrade your engine.

NOTE

- During the ServiceComb engine upgrade, the microservice and engine are intermittently disconnected, but services of running microservices are not affected. You are advised not to upgrade, restart, or change microservices when upgrading a ServiceComb engine.
- Version rollback is not supported after the upgrade.
- For details about the precautions for upgrading an exclusive ServiceComb engine from 1.x to 2.x, see **What Do I Need to Know Before Upgrading an Exclusive ServiceComb Engine?**

Background

During upgrade, two instances are upgraded in rolling mode without service interruptions. However, one of the two access addresses may be unavailable. In this case, you need to quickly switch to the other instance. Currently, ServiceComb SDK and Mesher support instance switching. If you call the APIs of the service center and configuration center for service registry and discovery, instance switching is required.

Upgrading a ServiceComb Engine Version

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Click **Upgrade** in the **Operation** column of the target engine. Alternatively, click the target engine and click **Upgrade** in the **ServiceComb Engine Information** area.

Step 5 Select **Target Version** and view the version description. Determine whether to upgrade the software to this version.

Step 6 Click **OK**.

If the upgrade fails, click **Retry** to perform the upgrade again.

----End

3.2.10 Deleting a ServiceComb Engine

You can delete an exclusive ServiceComb engine if it is no longer used.

NOTICE

- Deleted engines cannot be recovered. Exercise caution when performing this operation.
- For engine 1.x, if the cse_admin_trust agency is missing, deleting the engine will cause residual DNS, VPC, and security group resources on the tenant side. You need to delete them by yourself.

Background

You can delete exclusive ServiceComb engines in the following states:

- Available
- Unavailable
- Creation failed
- Resizing failed
- Upgrade failed

Deleting a ServiceComb Engine

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click **Delete** in the **Operation** column of the target engine. Alternatively, click the target engine and click **Delete** in the **ServiceComb Engine Information** area.

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

NOTE

If the deletion fails, click **Force Delete**.

----End

3.2.11 Changing ServiceComb Engine Specifications

Specifications of exclusive ServiceComb engines can be automatically changed online. The specifications can only be increased. The service will be disconnected intermittently during the change, which does not affect services. New services cannot be registered during the change.

Changing ServiceComb Engine Specifications

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click **More** > **Change Specifications** in the **Operation** column of the target engine. Alternatively, click the target engine and click **Change Specifications** in the **ServiceComb Engine Information** area.

Step 4 On the displayed page, select the target specifications.

Step 5 Click **Change Now**, confirm the information, and click **Submit**.

----End

3.2.12 Managing Security Authentication for a ServiceComb Engine

A ServiceComb engine may be used by multiple users. Different users must have different ServiceComb engine access and operation permissions based on their responsibilities and permissions. If security authentication is enabled for an exclusive ServiceComb engine, grant different access and operation permissions to users based on the roles associated with the accounts used by the users to access the ServiceComb engine.

For details about security authentication, see **System Management**.

Currently, Java chassis and Spring Cloud support security authentication for microservices. The Java chassis version must be 2.3.5 or later, and Spring Cloud must integrate Spring Cloud Huawei 1.6.1 or later.

You can enable or disable security authentication for the exclusive ServiceComb engine based on service requirements.

- **Enabling Security Authentication**

  If a ServiceComb engine is available with security authentication disabled, you can enable security authentication based on service requirements.

  After security authentication is enabled and programming interface authentication is also enabled, if security authentication parameters are not configured for the microservice components connected to the engine, or the security authentication account and password configured for the microservice components are incorrect, the heartbeat of the microservice components fails and the service is forced to go offline. Perform the following steps:

  – Spring Cloud: For details, see **Connecting Spring Cloud Applications to ServiceComb Engines**.

  – Java Chassis: For details, see **Connecting Java Chassis Applications to ServiceComb Engines**.

- **Disabling Security Authentication**

  If a ServiceComb engine is available with security authentication enabled, you can disable security authentication based on service requirements.

  After security authentication is disabled for a microservice component, service functions of the microservice component are not affected no matter whether security authentication parameters are configured for the microservice component.

Enabling Security Authentication

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 In the **Network Configuration and Security** area, click **Enable security authentication**.

- If the engine version is earlier than 1.2.0, go to **Step 5**.
- If the engine version is 1.2.0 or later, go to **Step 6**.

Step 5 Upgrade the engine to 1.2.0 or later.

1. Click **Upgrade**.
2. Select **Target Version** and view the version description. Determine whether to upgrade the software to this version. Then, click **OK**.
3. Select the upgraded ServiceComb engine. In the **Network Configuration and Security** area, click **Enable security authentication**.

Step 6 On the **System Management** page, enable security authentication.

- To enable security authentication for the first time, click **Enable security authentication**.

  You need to create user **root** first. Enter and confirm the password of user **root**. Then, click **Create Now**.
- Enable security authentication again and enter the name and password of the account associated with the **admin** role in the engine.

Step 7 (Optional) Create a role based on service requirements. For details, see **Roles**.

Step 8 (Optional) Create an account based on service requirements. For details, see **Accounts**.

Step 9 On the **System Management** page, click **Enable security authentication** and configure the security settings.

- If you enable **Authenticate Console**, go to **Step 11**.

  After **Authenticate Console** is enabled, you need to use an account and password to log in to the CSE console. The login user can only view and configure services on which the user has permission.
- If you enable **Authenticate Programming Interface**, go to **Step 10**.

  After **Authenticate Programming Interface** is enabled, **Authenticate Console** is automatically enabled.

  After it is enabled, you need to add the corresponding account and password to the microservice configuration file. Otherwise, the service cannot be registered with the engine.

  After it is disabled, you can register the service with the engine without configuring the account and password in the microservice configuration file, which improves the efficiency. You are advised to disable this function when accessing the service in a VPC.

Step 10 Configure the SDK. For microservice components that have been deployed but not configured with security authentication parameters, configure the account name and password for security authentication and then upgrade the component. For details, see **Configuring the Security Authentication Account and Password for a Microservice**.

Step 11 Click **OK**.

After the ServiceComb engine is updated and the engine status changes from **Configuring** to **Available**, security authentication is enabled successfully.

----End

Disabling Security Authentication

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 In the **Network Configuration and Security** area, click **Disable security authentication**.

Step 5 Click **OK**. After the ServiceComb engine is updated and the engine status changes from **Configuring** to **Available**, security authentication is disabled successfully.

NOTE

After security authentication is disabled, accounts created on the engine will not be deleted.

----End

3.2.13 Managing Tags

Tags facilitate ServiceComb engine identification and management.

If your organization has configured tag policies for ServiceComb engines, add tags to engines based on the policies. If a tag does not comply with the tag policies, engine creation may fail. Contact your administrator to learn more about tag policies.

You can add tags to a ServiceComb engine when creating the engine or add tags on the details page of the created engine. Up to 20 tags can be added to an engine. Tags can be modified and deleted.

A tag consists of a tag key and a tag value. **Table 3-5** lists the tag key and value requirements.

Table 3-5 Tag naming rules

Tag	Rule
Key	• Cannot be blank. • Must be unique for the same instance. • Contain a maximum of 128 characters. • Contain only letters, digits, spaces, and special characters (_ . : = + - @). • Cannot start with a space or **_sys_** or end with a space.

Tag	Rule
Value	● Contain a maximum of 255 characters. ● Contain only letters, digits, spaces, and special characters (_ . : = + - @).

Managing Tags

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine. The details page is displayed.

Step 4 In the **ServiceComb Engine Information** area, perform the following operations in the **Tag** field as required:

- Add a tag

  NOTICE

  Adding tags will affect engine services for about 10 seconds. Add tags during off-peak hours.

  a. Click **Tag Management**. The **Edit Tag** dialog box is displayed.

  b. Click ⊕ **Add Tag** and enter a tag key and value in the text boxes.

  c. Click **OK**.

- Modify a tag

  NOTICE

  Modifying tags will affect engine services for about 10 seconds. Modify tags during off-peak hours.

  a. Click **Tag Management**. The **Edit Tag** dialog box is displayed.

  b. You can modify the tag key and value in the original text boxes.

  c. Click **OK**.

- Delete a tag

  Click ⊖ in the row that contains the tag to be deleted. In the dialog box that is displayed, click **OK** to delete the tag.

----End

3.3 Using ServiceComb Engines

3.3.1 Using the Microservice Dashboard

You can view metrics related to microservices through the dashboard in real time. Based on abundant and real-time dashboard data, you can take corresponding governance actions for microservices.

NOTE

This function is supported by ServiceComb engine 1.x and 2.4.0 and later versions.

Background

- If a microservice application is deployed on ServiceStage, you need to configure the microservice engine during application deployment. The application automatically obtains the service registry and discovery address, configuration center address, and dashboard address. You do not need to configure the monitor address.
- If the microservice application is locally started and registered with the ServiceComb engine, manually configure the monitor address before using the dashboard.

  For details, see **Using Dashboard**.

Viewing Microservice Running Metrics

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Dashboard**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 On the **Dashboard** page, select an application from the drop-down list box and enter a microservice name in the search box. The operating metrics of the microservice are displayed.

Click **View Diagram** to view the description of operating metrics.

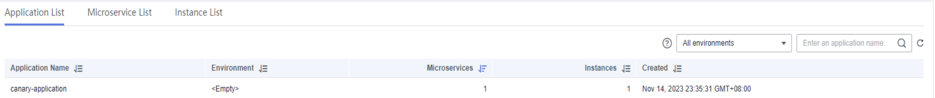
Step 7 Select a sorting order to sort the filtered microservices.

----End

3.3.2 Managing Microservices

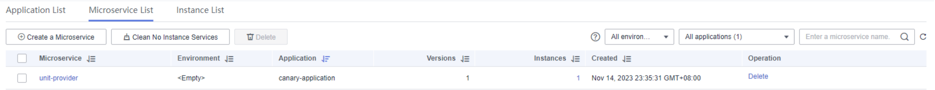
You can use the microservice catalog to view microservice details and search for target microservices to maintain microservices. The **Microservice Catalog** page contains the following tabs:

- **Application List**: displays all applications of the current ServiceComb engine. You can search for the target application by application name, or filter applications by environment. For details, see **Viewing the Application List**.



Application Name	Environment	Microservices	Instances	Created
canary-application	<Empty>	1	1	Nov 14, 2023 23:35:31 GMT+08:00

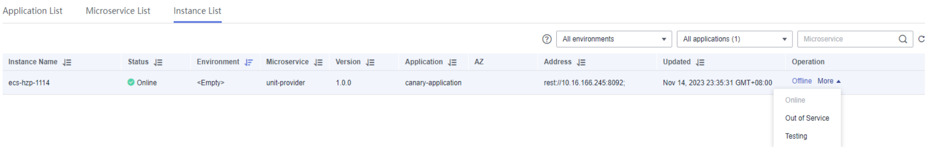
- **Microservice List**: For details about the operations supported by in **Microservice List**, see the following table.



□	Microservice	Environment	Application	Versions	Instances	Created	Operation
□	unit-provider	<Empty>	canary-application	1	1	Nov 14, 2023 23:35:31 GMT+08:00	Delete

Operation	Description
Viewing the Microservice List	Displays all microservices of the current ServiceComb engine. You can search for the target microservice by microservice name, or filter microservices by environment and application.
Viewing Microservice Details	On the microservice details page, you can view the instance list, called services, calling services, dynamic configuration, and service contract.
Creating a Microservice	Creates a microservice.
Cleaning Versions Without Instances	Cleans microservice versions that have no instances.
Deleting a Microservice	Deletes a microservice that is no longer used.
Dynamic Configuration	Creates a microservice-level configuration.
Dark Launch	In dark launch, new features are tested in a selected group of users. When the features become mature and stable, they are released to all users.

- **Instance List**: For details about the operations supported by in **Instance List**, see the following table.



Instance Name	Status	Environment	Microservice	Version	Application	AZ	Address	Updated	Operation
ecs-hzp-1114	Online	<Empty>	unit-provider	1.0.0	canary-application		rest://10.16.166.245:8092;	Nov 14, 2023 23:35:31 GMT+08:00	Offline More

Operation	Description
Viewing the Instance List	Displays all instances of the current ServiceComb engine. You can search for the target instance by microservice name, or filter instances by environment and application.
Changing the Instance Status	**Status** indicates the status of a microservice instance.

Viewing the Application List

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Catalog**.

- For engines with security authentication disabled, go to **Step 6**.
- For engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **Application List** to view details about all applications of the current account under the engine.

You can search for the target application by application name, or filter applications by environment.

----End

Viewing the Microservice List

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Catalog**.

- For engines with security authentication disabled, go to **Step 6**.
- For engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **Microservice List** to view all microservices of the current account under the engine.

You can search for the target microservice by microservice name, or filter microservices by environment and application.

----End

Viewing Microservice Details

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Catalog**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click the microservice to be viewed in **Microservice List**. On the displayed page, view the instance list, called services, calling services, configurations, and service contract.

----End

Creating a Microservice

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Catalog**.

- For engines with security authentication disabled, go to **Step 6**.
- For engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Choose **Microservice List** > **Create a Microservice** and set microservice parameters by referring to the following table. Parameters marked with an asterisk (*) are mandatory.

Parameter	Description
*Microservice	Microservice name, for example, **myServiceName**.
*Application	Name of the application to which the microservice belongs. Microservices are isolated by applications.
*Version	Microservice version. The default value is **1.0.0**. **NOTE** The microservice version is in the format of X.Y.Z or X.Y.Z.B, where X, Y, Z, and B are digits and range from 0 to 32767. The value contains 3 to 46 characters.
*Environment	Environment where the microservice is located to isolate microservice data, including the version and instance.
Detail	Microservice description.

Step 7 Click **OK**.

Once the microservice is created, it will be displayed in **Microservice List**.

----End

Cleaning Versions Without Instances

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Catalog**.

- For engines with security authentication disabled, go to **Step 6**.
- For engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Choose **Microservice List** > **Clean No Instance Services**. Select the microservice version without instances to be cleaned.

You can search for the target microservice by microservice name, or filter microservices by environment and application.

Step 7 Click **OK**.

----End

Deleting a Microservice

NOTICE

- After a microservice is deleted, you can restore it by referring to **Restoring Backup Data**.
- If the service to be deleted has instances, delete the instances first. Otherwise, the service will be registered again.

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Catalog**.

- For engines with security authentication disabled, go to **Step 6**.
- For engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **Microservice List**.

- To delete microservices in batches, select the microservices to be deleted and click **Delete** above the microservices.
- To delete one microservice, locate the row that contains the microservice to be deleted and click **Delete** in the **Operation** column.

Step 7 In the displayed dialog box, enter **DELETE** to confirm the deletion and click **OK**.

----End

Dynamic Configuration

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Catalog**.

- For engines with security authentication disabled, go to **Step 6**.
- For engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **Microservice List**.

Step 7 Click the target microservice.

Step 8 Choose **Dynamic Configuration**. On the **Dynamic Configuration** tab, perform the following operations.

NOTICE

Configuration items are stored in plaintext. Do not include sensitive data.

Operation	Procedure
Creating a configuration item	See **Creating a Microservice-Level Configuration**. **Microservice-level** is selected for **Configuration Range** and **Microservices** is set to the current microservice.
Viewing historical versions	Click **View Historical Version** in the **Operation** column of the target configuration item.
Disabling a Configuratio n Item	1. In the **Operation** column of the target configuration item, choose **More** > **Disable**. 2. Click **OK**.
Modifying a configuration item	1. Click **Edit** in the **Operation** column corresponding to the target configuration item. 2. On the configuration details page, click **Edit**. 3. On the **Configuration Details** tab, enter the new configuration. 4. Click **Save**.

Operation	Procedure
Deleting a configuration item	1. In the **Operation** column of the target configuration item, choose **More** > **Delete**. 2. Click **OK**.

----End

Dark Launch

In dark launch, new features are tested in a selected group of users. When the features become mature and stable, they are released to all users. This ensures the smooth feature rollout.

NOTE

- For microservices developed based on the ServiceComb Java Chassis framework, add dependency **darklaunch** or **handler-router** to POM and add **servicecomb.router.type=router** to the configuration file.
- For microservices developed based on the Spring Cloud Huawei framework, add dependency **spring-cloud-starter-huawei-router** to POM.

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Catalog**.

- For engines with security authentication disabled, go to **Step 6**.
- For engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 In the microservice list, click a microservice. On the displayed page, choose **Dark Launch**.

Step 7 Click **Add Launch Rule**.

- To add a launch rule by **Weight**:
  a. Click **Weight**.
  b. Set the following parameters.

Item	Description
Rule Name	Name of the rule.

Item	Description
Scope	■ Microservice version to which the rule applies. ■ Select **Do you want to add a customized version?** and add a new version as prompted.
Rule Configuration	Traffic allocation rate for the selected version. Traffic is evenly allocated to the selected service versions based on the configured value.

c. Click **OK** to complete the weight rule configuration and dark launch.

- To add a launch rule by **Customization**:

NOTE

Dark launch rules can be delivered only after dark launch is implemented for microservices developed based on the ServiceComb Java Chassis framework using dependency **darklaunch** and microservices developed based on the Spring Cloud Huawei framework. Dark launch rules that depend on **handler-router** need to be manually delivered in the configuration center.

a. Click **Custom**.

b. Set the following parameters.

Item	Description
Rule Name	Name of the rule.
Scope	■ Microservice version to which the rule applies. ■ Select **Do you want to add a customized version?** and add a new version as prompted.

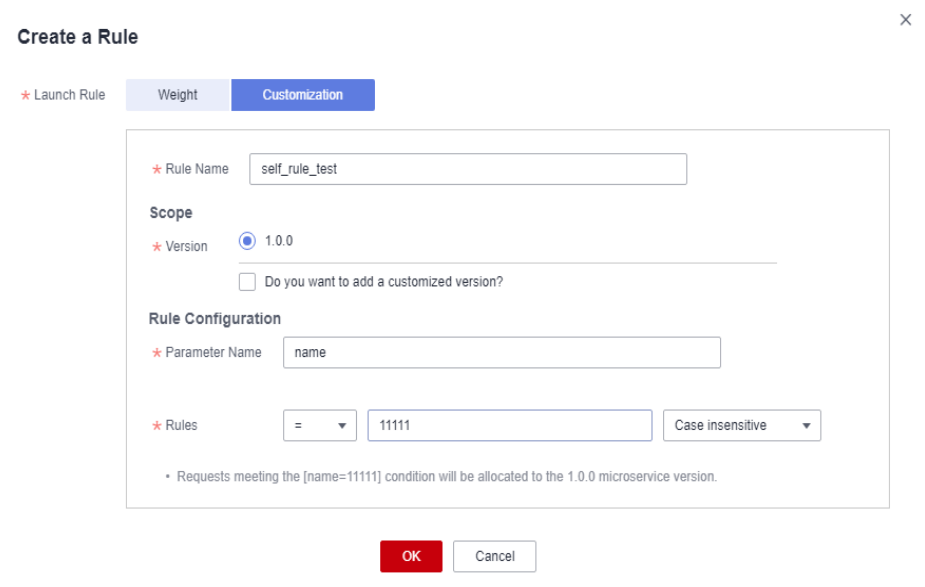
Item	Description
Rule Configuration	Configure the matching rule. When **darklaunch** is used to implement dark launch, this parameter configures **policyCondition**. Otherwise, it configures **Headers**. ■ Parameter Name Set this parameter based on the parameter name of contract or the customized key of the header. ■ Rules By selecting the matching character and the value corresponding to the key of contract or the key of the header, requests that meet the rules are allocated to the microservice version. **NOTE** ○ If **~** is selected from the drop-down list next to **Rules**, the asterisk (*) and question mark (?) in the **Rules** value can be used for fuzzy matching. The asterisk (*) indicates a character of any length, and the question mark (?) indicates one character. For example, if the rule value of **Name** is set to ***1000**, all **Name** fields ending with 1000 can be matched. ○ If **~** is not selected from the drop-down list next to **Rules**, the asterisk (*) and question mark (?) in the **Rules** value cannot be used for fuzzy matching.

c. Click **OK** to complete the customization rule configuration and dark launch.

----End

Examples of delivering dark launch rules:

- For microservices developed based on the ServiceComb Java Chassis framework, rules are delivered based on dependency **darklaunch** on the ServiceComb engine page. You can add dark launch rules in customized mode.



Create a Rule

* Launch Rule: Weight | **Customization**

* Rule Name: self_rule_test

Scope

* Version: ● 1.0.0

□ Do you want to add a customized version?

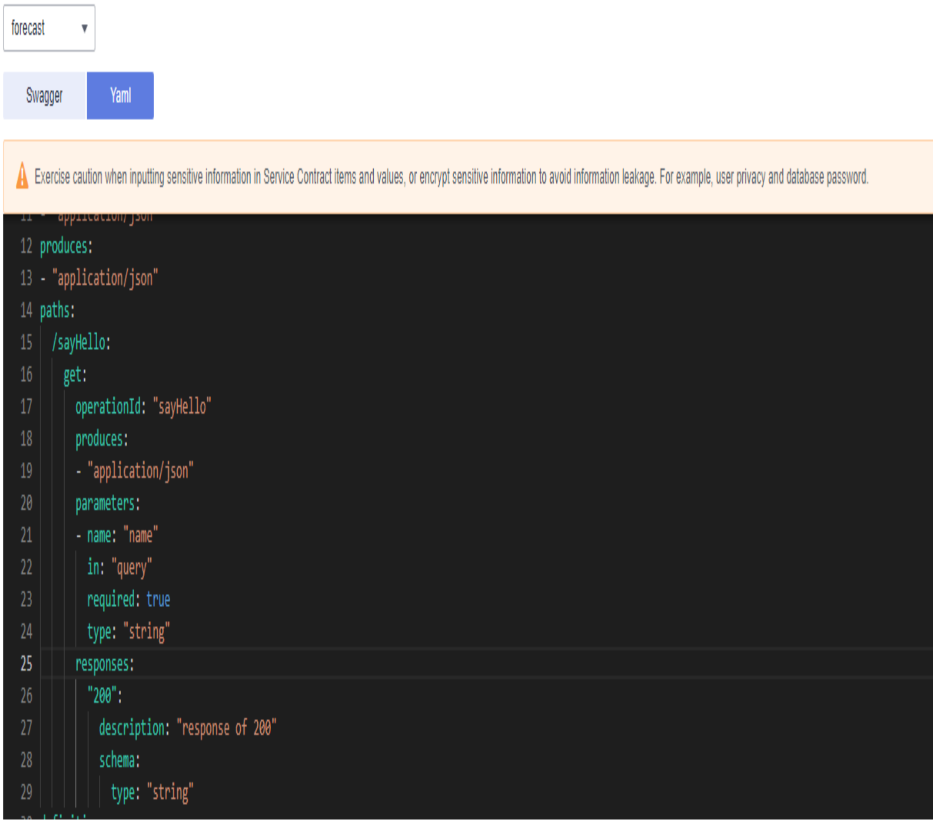
Rule Configuration

* Parameter Name: name

* Rules: = | 11111 | Case insensitive

- Requests meeting the [name=11111] condition will be allocated to the 1.0.0 microservice version.

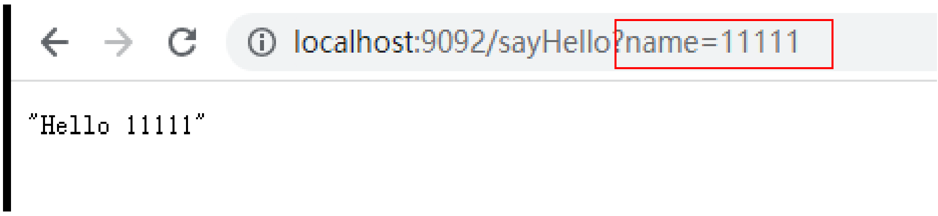
This key must exist in the contract. It is possible that the server API is **String paramA**, but **paramB** is actually generated after the annotation is added. Therefore, **paramB** should be set here.



Exercise caution when inputting sensitive information in Service Contract items and values, or encrypt sensitive information to avoid information leakage. For example, user privacy and database password.

```
produces:
- "application/json"
paths:
  /sayHello:
    get:
      operationId: "sayHello"
      produces:
      - "application/json"
      parameters:
      - name: "name"
        in: "query"
        required: true
        type: "string"
      responses:
        "200":
          description: "response of 200"
          schema:
            type: "string"
```

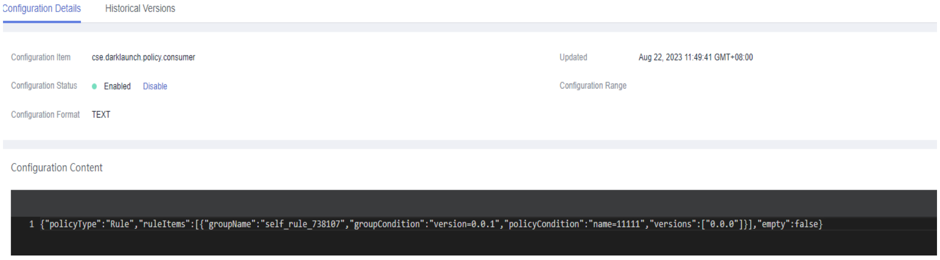
By selecting the matching character and the value corresponding to the key of contract, requests that meet the rules are allocated to the microservice version.



localhost:9092/sayHello?name=11111

```
"Hello 11111"
```

A delivered rule is as follows. The configuration item is **cse.darklaunch.policy.***${serviceName}*.



Configuration Item: cse.darklaunch.policy.consumer

Updated: Aug 22, 2023 11:49:41 GMT+08:00

Configuration Status: ● Enabled Disable

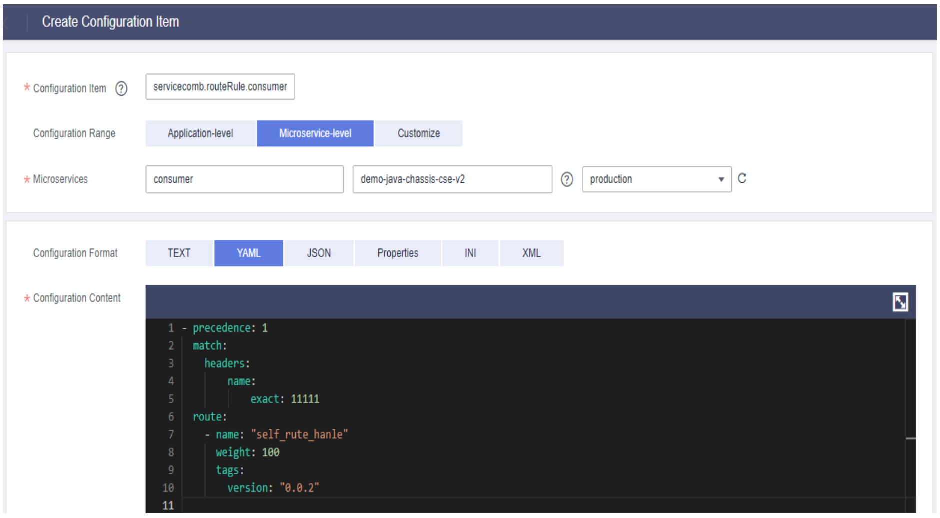
Configuration Range:

Configuration Format: TEXT

Configuration Content

```
{"policyType":"Rule","ruleItems":[{"groupName":"self_rule_738107","groupCondition":"version=0.0.1","policyCondition":"name=11111","versions":["0.0.0"]}],"empty":false}
```

- For microservices developed based on the ServiceComb Java Chassis framework, dark launch rules that depend on **handler-router** need to be manually delivered in the configuration center. The configuration item is **servicecomb.routeRule.***${serviceName}*. The content is as follows:



* Configuration Item: servicecomb.routeRule.consumer

Configuration Range: Application-level | Microservice-level | Customize

* Microservices: consumer | demo-java-chassis-cse-v2 | production

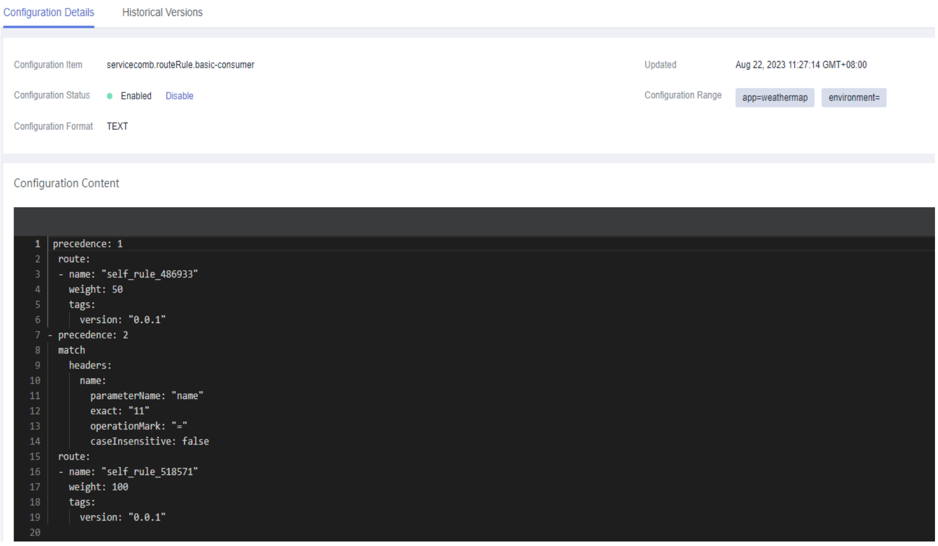
Configuration Format: TEXT | YAML | JSON | Properties | INI | XML

* Configuration Content

```yaml
- precedence: 1
  match:
    headers:
        name:
            exact: 11111
  route:
    - name: "self_rute_hanle"
      weight: 100
      tags:
        version: "0.0.2"

```

- For microservices developed based on the Spring Cloud Huawei framework, dark launch rules delivered on the ServiceComb engine page are as follows:



Configuration Item servicecomb.routeRule.basic-consumer

Updated Aug 22, 2023 11:27:14 GMT+08:00

Configuration Status ● Enabled

Configuration Range app=weathermap environment=

Configuration Format TEXT

Configuration Content

```
precedence: 1
 route:
 - name: "self_rule_486933"
   weight: 50
   tags:
     version: "0.0.1"
- precedence: 2
 match
   headers:
     name:
       parameterName: "name"
       exact: "11"
       operationMark: "="
       caseInsensitive: false
 route:
 - name: "self_rule_518571"
   weight: 100
   tags:
     version: "0.0.1"

```

Viewing the Instance List

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Catalog**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **Instance List** to view all instances of the engine.

You can search for the target instance by microservice name, or filter instances by environment and application.

----End

Changing the Instance Status

Status indicates the status of a microservice instance.

NOTE

The status of microservice instances synchronized by binding ServiceComb engines cannot be changed during component creation and deployment by referring to **Creating and Deploying a Component**.

The following table describes the microservice instance statuses.

Status	Description
Online	The instance is running and can provide services.
Offline	Before the instance process ends, the instance is marked as not providing services externally.
Out of Service	The instance has been registered with the ServiceComb engine and does not provide services.
Testing	The instance is in the internal joint commissioning state and does not provide services.

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Catalog**.

- For engines with security authentication disabled, go to **Step 6**.
- For engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **Instance List**, select the target instance, and change the instance status.

- Offline

  In the **Operation** column, click **Offline**.
- Online

  In the **Operation** column, choose **More** > **Online**.
- Out of Service

  In the **Operation** column, choose **More** > **Out of Service**.
- Testing

  In the **Operation** column, choose **More** > **Testing**.

----End

3.3.3 Service Scenario Governance

ServiceComb engines provide unified traffic feature governance based on dynamic configurations for different microservice development frameworks, such as Spring

Cloud and Java chassis. You can use the microservice governance function of CSE by introducing related governance components to the development frameworks.

ServiceComb engine governance consists of two steps: creating a service scenario and creating a governance policy. The two steps can be performed before microservice deployment for independent governance planning.

NOTE

- This section applies to ServiceComb engine 2.x.
- If the ServiceComb engine version is 2.0.0 or later but earlier than 2.4.0, the name of this section is "Microservice Governance".

Prerequisites

- You need to understand the API design of the microservice to be governed and create service scenarios based on the API features.
- You need to enable the dynamic configuration-based traffic feature governance function for the development framework of the microservice to be governed. If the function is not enabled, the microservice governance function can still be used, but the governance has no effects.

Governance Policies

You can configure the following policies: Rate Limiting, Circuit Breaker, Retry, and Bulkhead. For details, see the following table.

Policy	Description
Rate Limiting	In the case of a traffic storm or predictable traffic spikes, rate limiting is performed on non-key service scenarios to prevent service and data breakdown caused by instantaneous heavy traffic.
Retry	When a service encounters a non-fatal error (such as occasional timeout), retries can be performed to prevent service failures.
Bulkhead	In the case of a large-scale concurrent traffic storm or predictable traffic impact, the concurrent traffic is controlled to prevent service and data breakdown caused by instantaneously large concurrent traffic.
Circuit Breaker	When the error rate of a service scenario exceeds the threshold, all requests in the service scenario will be rejected within one minute to ensure the availability of the entire service system. Then 50% of the service requests will be accepted and statistics on the service error rate will be collected until the error rate in the service scenario is reduced to a value lower than the threshold.

Creating a Service Scenario

NOTE

When a service scenario is created, the configuration starting with **servicecomb.matchgroup.** is automatically generated.

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Service Scenario Governance**.

NOTE

If the ServiceComb engine version is 2.0.0 or later but earlier than 2.4.0, choose **Microservice Governance**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Choose **Service Scenarios** > **Create Service Scenario** and set parameters by referring to the following table.

Parameter	Description
Scenario	Enter the service scenario name.
Environment	Select a microservice environment.
Application	Select the application to which the service scenario to be created belongs.
Matching Rule	Click **Add Matching Rule** to set the request marker. ● **Method**: Select the method of marking the traffic request feature. The **GET**, **PUT**, **POST**, **DELETE**, and **PATCH** methods are supported. ● **Path**: Set features contained in the traffic request URI. ● **Headers**: Click **Add Headers Rule** and set the marker of the traffic request header. NOTE ● **Method** and **Path** are mandatory. ● **Headers** is optional.

Step 7 Click **OK**.

NOTE

- Click ⊞ in the row that contains a service scenario to view the matching rule details.
- Click **Edit** in the **Operation** column of a service scenario to edit the service scenario.
- Click **Delete** in the **Operation** column of a service scenario to delete the service scenario.

----End

Creating a Governance Policy

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Service Scenario Governance**.

NOTE

If the ServiceComb engine version is 2.0.0 or later but earlier than 2.4.0, choose **Microservice Governance**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Go to the **Governance Policy** page and click **Create Governance Policy**.

Step 7 Select a governance mode, click **Create Policy**, and set parameters.

- Rate Limiting

Parameter	Description
Policy	Enter the name of the governance policy.
Service Scenarios	Set the service scenarios to which the governance policy applies. – Click **Select Service Scenario** and select the created service scenario. – Click **Create Service Scenario** to **create a service scenario**.
Requests per Unit	Set the number of requests and time segment. When the number of requests sent by the rate limiting object to the current service instance within the specified period exceeds the specified value, the excess requests are limited and error code 429 is returned.

- Retry

Parameter	Description
Policy	Enter the name of the governance policy.
Service Scenarios	Set the service scenarios to which the governance policy applies. – Click **Select Service Scenario** and select the created service scenario. – Click **Create Service Scenario** to **create a service scenario**.
Response Error Code	Enter response error codes to define the error types that trigger retries.
Retry Attempts	Set the number of retries.
Retry Interval	Select a retry policy. – **Fixed**: The retry interval is fixed. – **Exponential**: Each interval is selected by the exponential backoff algorithm.
Interval Duration	Set the retry interval duration. – If **Retry Interval** is set to **Fixed**, set the fixed interval. – If **Retry Interval** is set to **Exponential**, set the retry benchmark time and unit (s/ms).

- Bulkhead

Parameter	Description
Policy	Enter the name of the governance policy.
Service Scenarios	Set the service scenarios to which the governance policy applies. – Click **Select Service Scenario** and select the created service scenario. – Click **Create Service Scenario** to **create a service scenario**.
Max. Concurrency	Set the maximum number of concurrent requests based on the actual service processing capability of the system.
Block Duration	Set the block duration and unit (s/ms). When the number of concurrent requests exceeds the maximum, the requests are discarded after the blocking duration.

- Circuit Breaker

Parameter		Description
Policy		Enter the name of the governance policy.
Service Scenarios		Set the service scenarios to which the governance policy applies. – Click **Select Service Scenario** and select the created service scenario. – Click **Create Service Scenario** to **create a service scenario**.
Coverage	Sliding Window Type	Select a sliding window type. – **Time**: time window – **Requests**: request window
	Sliding Window Size	Set the size of the sliding window. – If **Sliding Window Type** is set to **Time**, the calls in the last n seconds or minutes are recorded and collected. – If **Sliding Window Type** is set to **Requests**, the latest n calls are recorded and collected. n is the size of the sliding window.
	Calls Baseline	Set the baseline of the number of calls, that is, the minimum number of calls required for collecting statistics on the call error rate. For example, if **Calls Baseline** is set to **10**, at least 10 call must be recorded to collect statistics on the error rate.
Triggers	Error Threshold	Percentage of call errors. This parameter is valid when **Set circuit breaker to trigger at an error threshold** is selected. When the call error rate is greater than or equal to the error threshold, circuit breaker occurs and response code 429 is returned.
	Slow Request Ratio	This parameter is valid when **Set circuit breaker to trigger at a specific request speed and ratio** is selected. Set the following parameters: – **Slow Speed**: defines the slow request threshold. If the response time of a request exceeds the threshold, the request is a slow request. – **Slow Threshold**: When the specified slow request ratio is reached, circuit breaker occurs and response code 429 is returned.

Step 8 Click **Create** to make the governance policy take effect.

NOTE

In the governance policy list, click ⊞ in the row where the service scenario is located:

- Click **Enable** in the **Operation** column of a governance policy to enable the policy.
- Click **Disable** in the **Operation** column of a governance policy to disable the policy.
- Click **Edit** in the **Operation** column of a governance policy to edit the policy.
- Click **Delete** in the **Operation** column of a governance policy to delete the policy.

----End

3.3.4 Microservice Governance

3.3.4.1 Overview

If an application is developed using the microservice framework, the microservice is automatically registered with the corresponding ServiceComb engine after the application is managed and started. You can perform service governance on the engine console by referring to **Governing Microservices**.

NOTE

This function is supported by ServiceComb engine 1.x and 2.4.0 and later versions.

3.3.4.2 Governing Microservices

After a microservice is deployed, you can govern it based on its running statuses.

Prerequisites

- You can create a microservice in **Microservice List** from **Service Catalog** and start the microservice. After the microservice starts, the service instance is registered under the corresponding service based on configurations in the **.yaml** file.
- If the microservice is not created in advance or has been deleted, the microservice is automatically created when the service instance is registered.
- After a microservice is created, register the service instance before performing the corresponding operation.

Governance Policies

You can configure the following policies: Load Balancing, Rate Limiting, Fault Tolerance, Service Degradation, Circuit Breaker, Fault Injection, and Blacklist and Whitelist. For details, see the following table.

Name	Description
Load Balancing	● Application scenario Generally, multiple instances are deployed for a microservice. Load balancing controls the policy for a microservice consumer to access multiple instances of a microservice provider to balance traffic. It includes polling, random, response time weigh, and session stickiness. ● For details about the configuration example of the governance policy and how to add dependencies to POM, see **Load Balancing**.
Rate Limiting	● Application scenario This policy controls the number of requests for accessing microservices to prevent the system from being damaged due to traffic impact. ● For details about the configuration example of the governance policy and how to add dependencies to the POM, see **Rate Limiting**.
Service Degradation	● Application scenario When a microservice invokes other microservices, the default value is forcibly returned or an exception is thrown instead of sending the request to the target microservice. In this way, the access to the target microservice is shielded and the pressure on the target microservice is reduced. ● For details about the configuration example of the governance policy and how to add dependencies to the POM, see **Service Degradation**.
Fault Tolerance	● Application scenario If an exception occurs when a microservice consumer accesses a provider, for example, the instance network is disconnected, the request needs to be forwarded to another available instance. Fault tolerance is often referred to as retry. ● For details about the configuration example of the governance policy and how to add dependencies to POM, see **Fault Tolerance**.
Circuit Breaker	● Application scenario If an exception occurs when a microservice consumer accesses a provider, for example, the instance network is disconnected or the request times out, and the exception accumulates to a certain extent, the consumer needs to stop accessing the provider and return an exception or a default value to prevent the avalanche effect. Automatic circuit breaker is supported, which determines a circuit breaker according to the error rate. ● For details about the configuration example and how to add dependencies to the POM, see **Circuit Breaker**.

Name	Description
Fault Injection	- Application scenario Fault injection can simulate an invoking failure, which is mainly used for function verification and fault scenario demonstration. - Governance of microservices connected to the Java Chassis development framework. For details about the configuration example of the governance policy and how to add dependencies to POM, see **Fault Injection**. **NOTE** This policy applies only to microservices accessed through Java chassis.
Blacklist and Whitelist	- Application scenario Based on the public key authentication mechanism, ServiceComb engines provide the blacklist and whitelist functions. The blacklist and whitelist can be used to control which services can be accessed by microservices. - Governance of microservices accessed through Java chassis The blacklist and whitelist take effect only after public key authentication is enabled. For details, see **Configuring Public Key Authentication**. **NOTE** This policy applies only to microservices accessed through Java chassis.

Configuring Load Balancing

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Governance**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

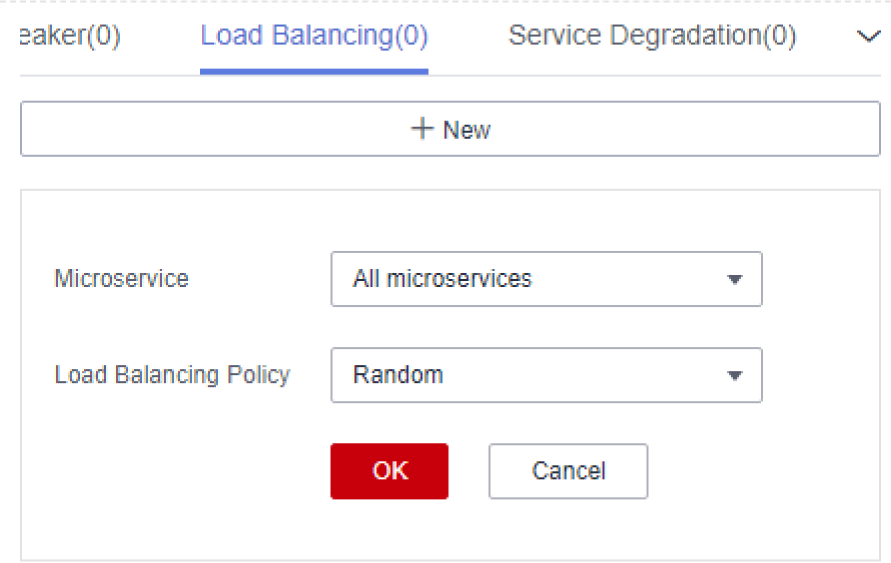
- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click the microservice to be governed.

Step 7 Choose **Load Balancing**.

Step 8 Click **New**. Select the microservices to be governed and select a proper load balancing policy. For details, see the following table.

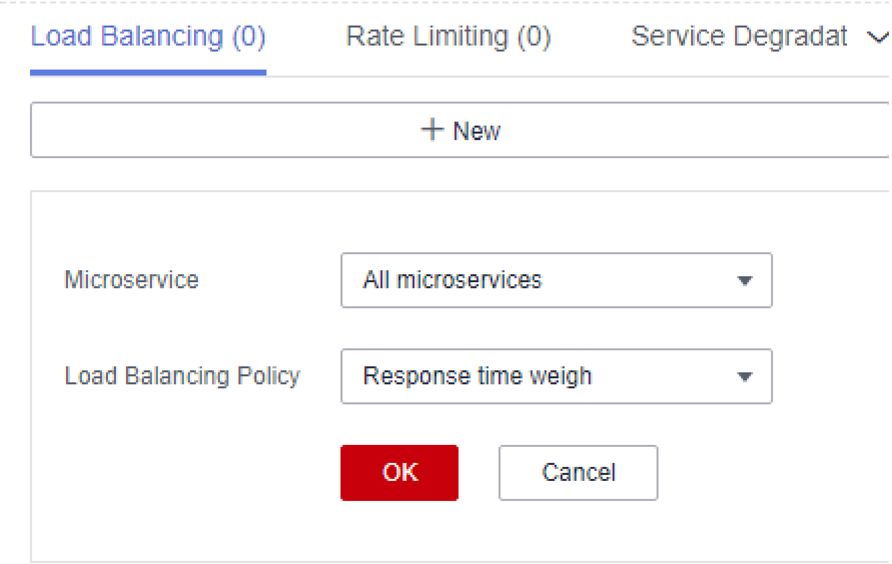
Figure 3-1 Configuring load balancing (for microservices accessed through Spring Cloud)



Microservice: All microservices

Load Balancing Policy: Random

Figure 3-2 Configuring load balancing (for microservices accessed through Java chassis)



Microservice: All microservices

Load Balancing Policy: Response time weigh

Policy	Description
Round robin	Supports routes according to the location information about service instances.
Random	Provides random routes for service instances.

Policy	Description
Response time weight	Provides weight routes with the minimum active number (latency) and supports service instances with slow service processing in receiving a small number of requests to prevent the system from stopping response. This load balancing policy is suitable for applications with low and stable service requests. **NOTE** This policy applies to microservices accessed through Java chassis.
Session stickiness	Provides a mechanism on the load balancer. In the specified session stickiness duration, this mechanism allocates the access requests related to the same user to the same instance. ● **Stickiness Duration**: time limit for keeping a session. The value ranges from 0 to 86400, in seconds. ● **Failures**: number of access failures. The value ranges from 0 to 10. If the upper limit of failures or the session stickiness duration exceeds the specified values, the microservice stops accessing this instance. **NOTE** This policy applies to microservices accessed through Java chassis.

Step 9 Click **OK**.

----End

Configuring Rate Limiting

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Governance**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

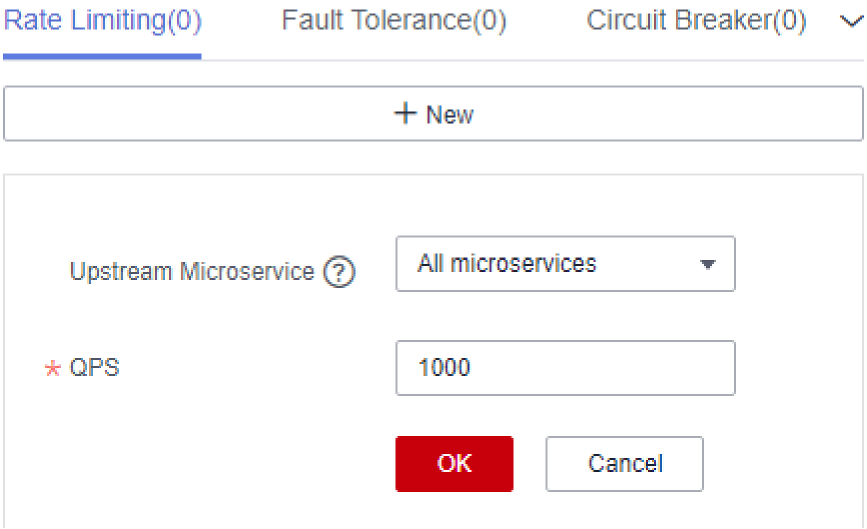
- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click the microservice to be governed.

Step 7 Click **Rate Limiting**.

Step 8 Click **New**. The following table describes configuration items of rate limiting.

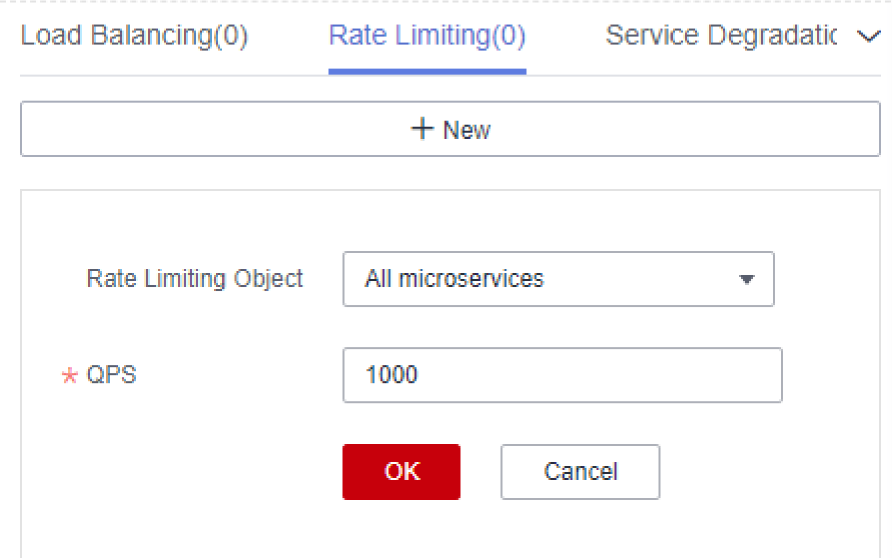
Figure 3-3 Configuring rate limiting (for microservices accessed through Spring Cloud)



Upstream Microservice: All microservices

* QPS: 1000

Figure 3-4 Configuring rate limiting (for microservices accessed through Java chassis)



Rate Limiting Object: All microservices

* QPS: 1000

Configuration Item	Description	Value Range
Rate Limiting Object	Other microservices that access the microservice. **NOTE** This configuration applies to microservices accessed through Java chassis.	Select an item from the drop-down list next to **Rate Limiting Object**.

Configuration Item	Description	Value Range
Upstream Microservice	Configure rate limiting for the upstream microservice to invoke the service. **NOTE** This configuration applies to microservices accessed through Spring Cloud.	Select an item from the drop-down list next to **Upstream Microservice**.
QPS	Requests generated per second. When the number of requests sent by the rate limiting object to the current service instance exceeds the specified value, the current service instance no longer accepts requests from the rate limiting object.	Enter an integer ranging from 1 to 99999.

NOTE

If a microservice has three instances, the rate limiting of each instance is set to 2700 QPS, then the total QPS is 8100, and rate limiting is triggered only when the QPS exceeds 8100.

Step 9 Click **OK**.

----End

Configuring Service Degradation

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Governance**.

- For engines with security authentication disabled, go to **Step 6**.
- For engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

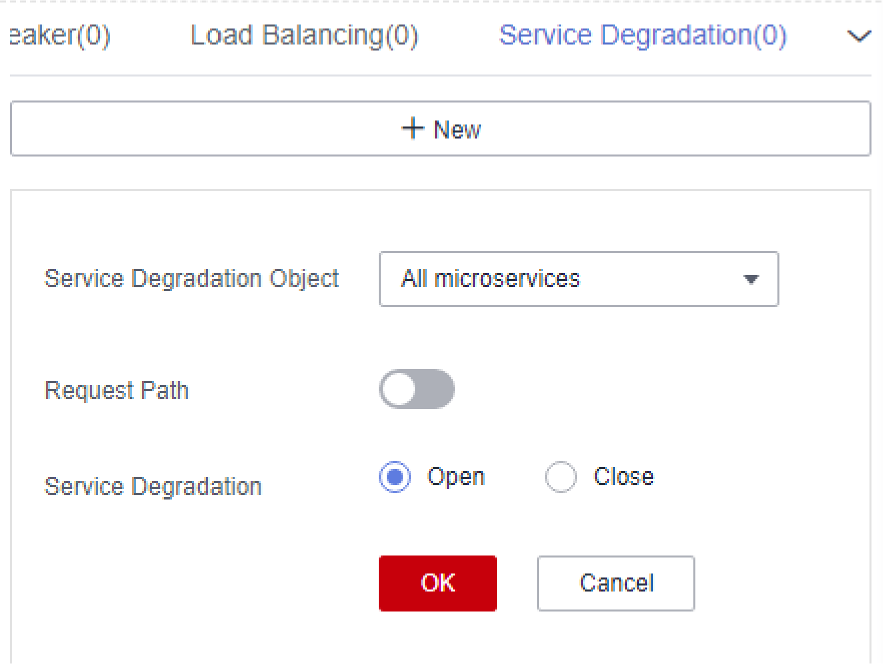
- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click the microservice to be governed.

Step 7 Click **Service Degradation**.

Step 8 Click **New** and select a proper policy. The following table describes the configuration items of service degradation.

Figure 3-5 Configuring service degradation (for microservices accessed through Spring Cloud)

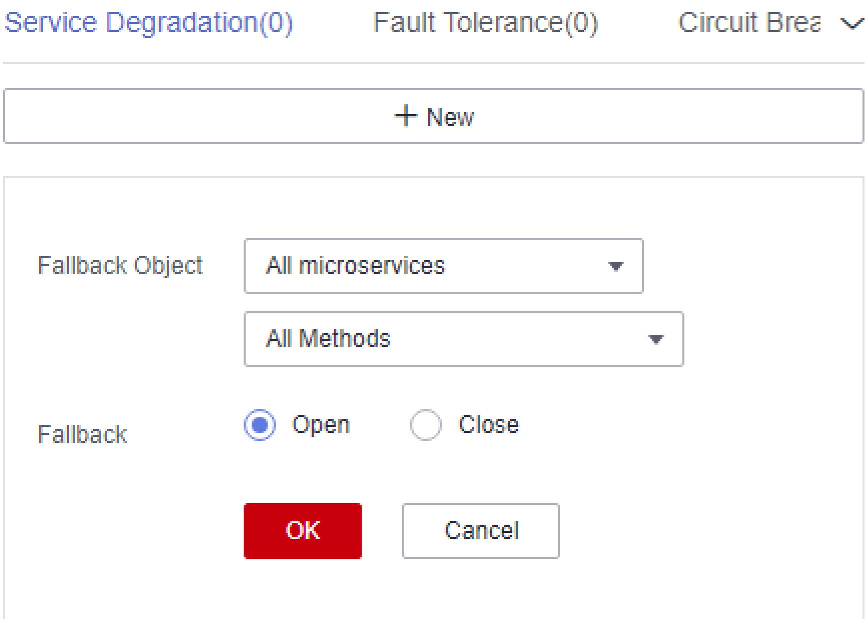


Service Degradation Object: All microservices

Request Path: off

Service Degradation: ● Open ○ Close

Figure 3-6 Configuring service degradation (for microservices accessed through Java chassis)



Fallback Object: All microservices

All Methods

Fallback: ● Open ○ Close

Configuration Item	Description
Fallback Object	Microservice to be degraded.
Request Path	Click and set **Method**, **Path**, and **Headers** to specify the request path. **NOTE** This configuration applies to microservices accessed through Spring Cloud.
Fallback	● Open ● Close

Step 9 Click **OK**.

----End

Configuring Fault Tolerance

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Governance**.

- For engines with security authentication disabled, go to **Step 6**.
- For engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

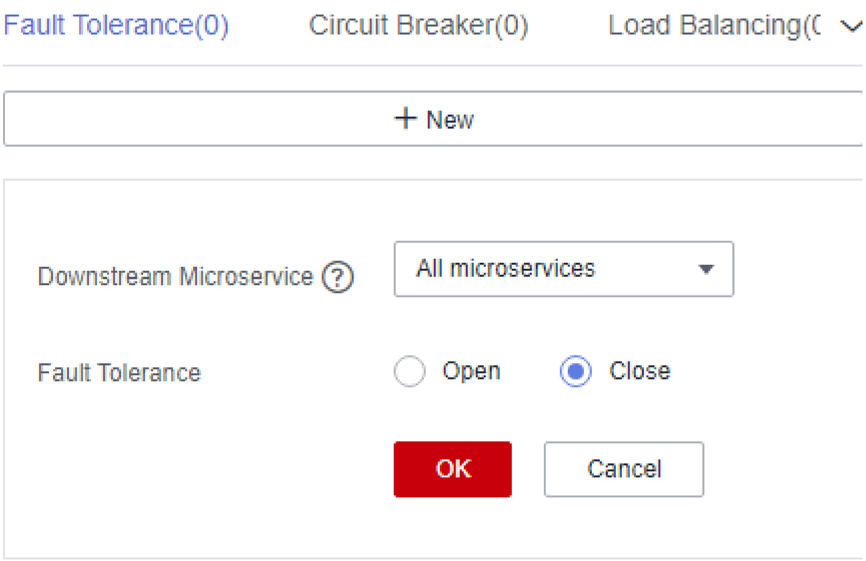
- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click the microservice to be governed.

Step 7 Click **Fault Tolerance**.

Step 8 Click **New** and select a proper policy. The following table describes the configuration items of fault tolerance.

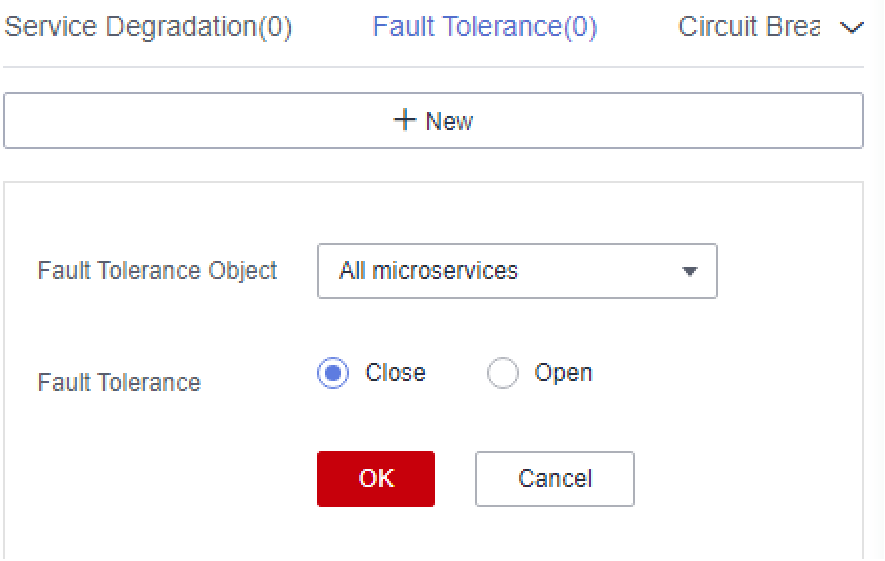
Figure 3-7 Configuring fault tolerance (for microservices accessed through Spring Cloud)



Downstream Microservice: All microservices

Fault Tolerance: ○ Open ● Close

Figure 3-8 Configuring fault tolerance (for microservices accessed through Java chassis)



Fault Tolerance Object: All microservices

Fault Tolerance: ● Close ○ Open

Configuration Item	Description
Downstream Microservice	Configure fault tolerance for the microservice to invoke the downstream microservice. You can select a value from the drop-down list. **NOTE** This configuration applies to microservices accessed through Spring Cloud.

Configuration Item	Description
Fault Tolerance Object	Microservice or method that the application relies on. **NOTE** This configuration applies to microservices accessed through Java chassis.
Fault Tolerance	**Open**: The system processes a request sent to the fault tolerance object based on the selected fault tolerance policy when the request encounters an error. **Close**: The system waits until the timeout interval expires and then returns the failure result even though the service request fails to be implemented.
FT Policy	This parameter is mandatory when **Fault Tolerance** is set to **Open**. For microservices accessed through Spring Cloud, set the following parameters: ● Number of attempts to the same microservice instance ● Number of attempts to the new microservice instance For microservices accessed through Java chassis, set the following parameters: ● Failover The system attempts to reestablish connections on different servers. ● Failfast The system does not attempt to reestablish a connection. After a request fails, a failure result is returned immediately. ● Failback The system attempts to reestablish connections on the same server. ● custom – Number of attempts to reestablish connections on the same server – Number of attempts to reestablish connections on new servers

Step 9 Click **OK**.

----End

Configuring Circuit Breaker

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Governance**.

- For engines with security authentication disabled, go to **Step 6**.
- For engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

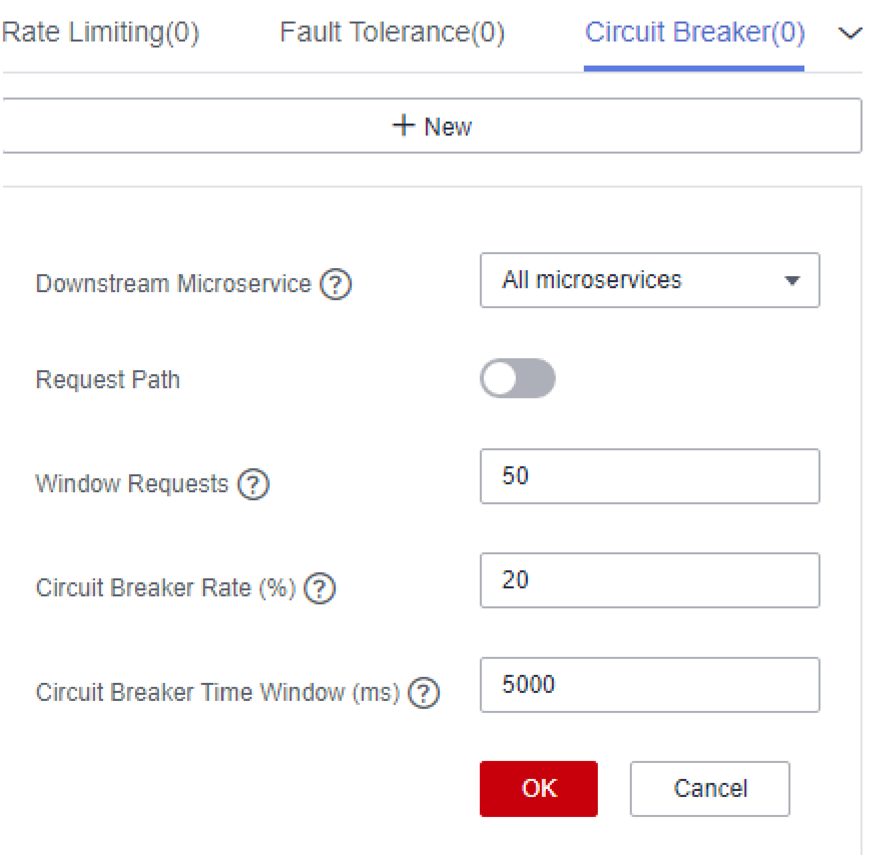
- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click the microservice to be governed.

Step 7 Click **Circuit Breaker**.

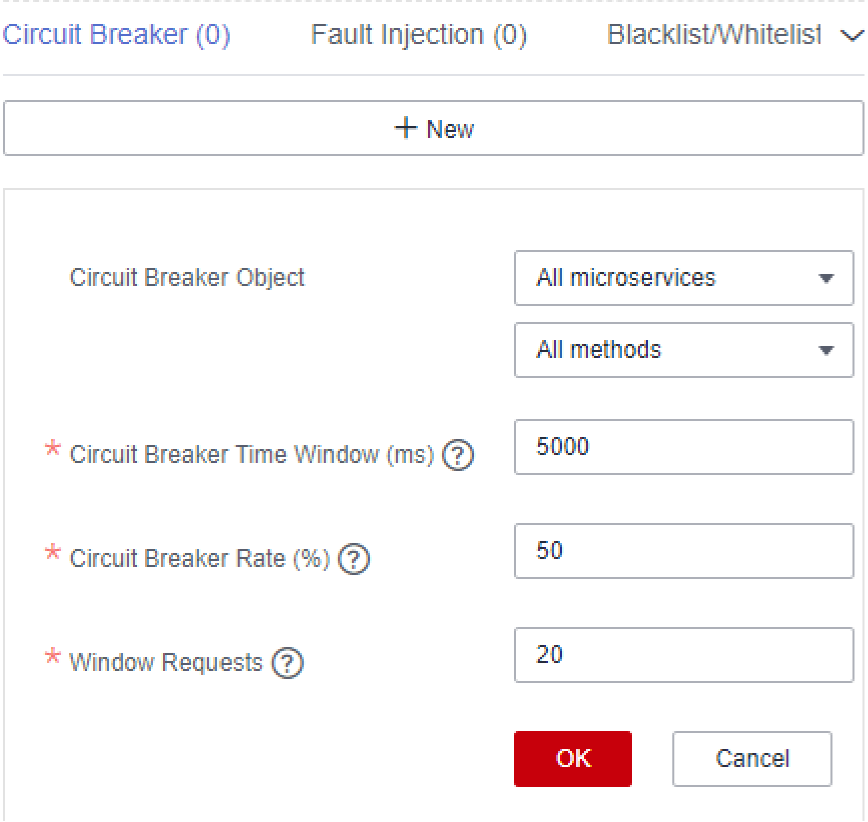
Step 8 Click **New** and select a proper policy. The following table describes the configuration items of circuit breaker.

Figure 3-9 Configuring circuit breaker (for microservices accessed through Spring Cloud)



Downstream Microservice	All microservices
Request Path	
Window Requests	50
Circuit Breaker Rate (%)	20
Circuit Breaker Time Window (ms)	5000

Figure 3-10 Configuring circuit breaker (for microservices accessed through Java chassis)



Circuit Breaker Object: All microservices; All methods

* Circuit Breaker Time Window (ms): 5000

* Circuit Breaker Rate (%): 50

* Window Requests: 20

Configuration Item	Description
Downstream Microservice	Configure circuit breaker for the microservice to invoke the downstream microservice. **NOTE** This configuration applies to microservices accessed through Spring Cloud.
Circuit Breaker Object	Microservice or method invoked by the application. **NOTE** This configuration applies to microservices accessed through Java chassis.
Request Path	Click ○ and set **Method**, **Path**, and **Headers** to specify the request path. **NOTE** This configuration applies to microservices accessed through Spring Cloud.
Triggering Condition	● **Circuit Breaker Time Window**: circuit breaker duration. The system does not respond to requests within this time window. ● **Request Failure Rate**: failure rate of window requests. ● **Window Requests**: number of requests received by the window. Circuit breaker is triggered only when **Request Failure Rate** and **Window Requests** both reach their thresholds.

Step 9 Click **OK**.

----End

Configuring Fault Injection

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Governance**.

- For engines with security authentication disabled, go to **Step 6**.
- For engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

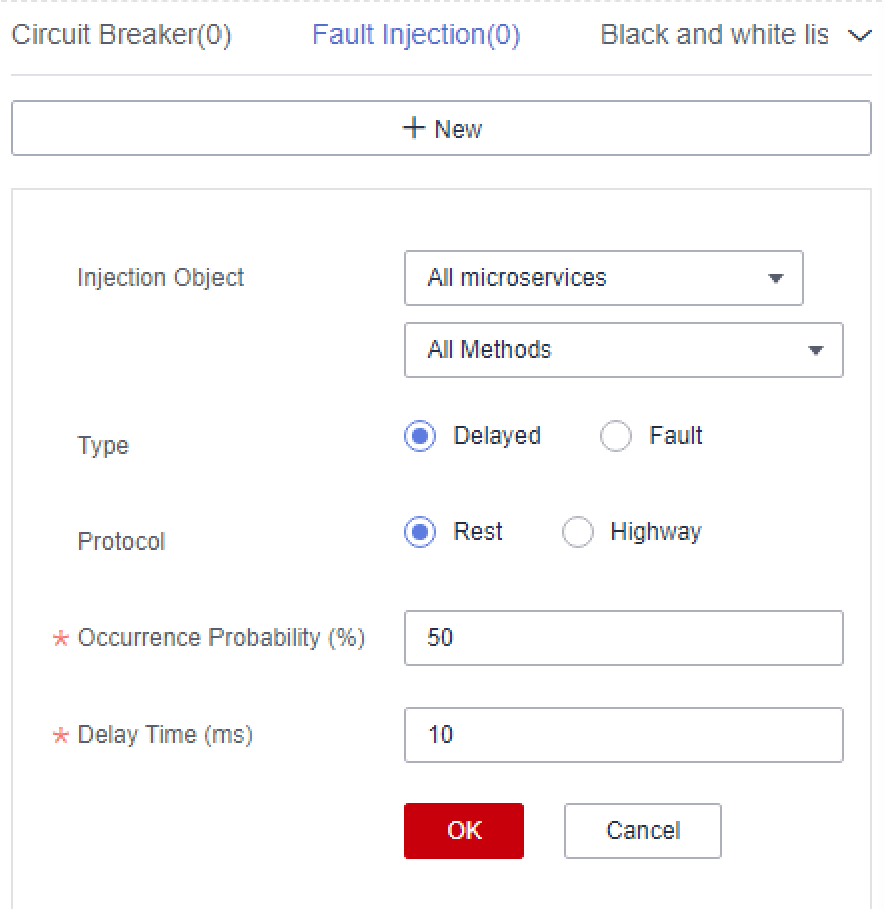
- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click the microservice to be governed.

Step 7 Click **Fault Injection**.

Step 8 Click **New** and select a proper policy. The following table describes the configuration items of fault injection.

Figure 3-11 Configuring fault injection (delayed)



Injection Object: All microservices; All Methods

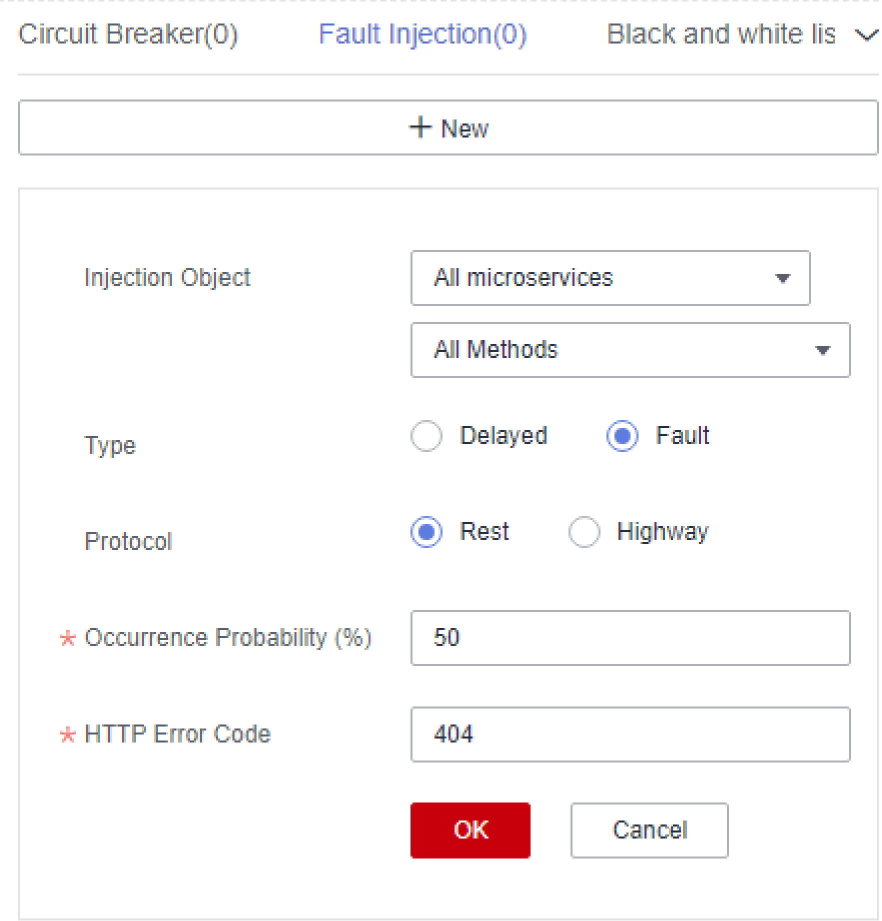
Type: ● Delayed ○ Fault

Protocol: ● Rest ○ Highway

* Occurrence Probability (%): 50

* Delay Time (ms): 10

Figure 3-12 Configuring fault injection (fault)



Injection Object: All microservices; All Methods

Type: ○ Delayed ● Fault

Protocol: ● Rest ○ Highway

* Occurrence Probability (%): 50

* HTTP Error Code: 404

Configuration Item	Description
Injection Object	Microservices for which fault injection is required. You can specify a method for this configuration item.
Type	Type of the fault injected to the microservice. ● Delayed ● Fault
Protocol	Protocol for accessing the microservice when latency or fault occurs. ● Rest ● Highway
Occurrence Probability	Probability of latency or fault occurrence.
Delay Time	Duration of the latency during microservice access. This parameter is required when **Type** is set to **Delayed**.

Configuration Item	Description
HTTP Error Code	HTTP error code during microservice access. This parameter is required when **Type** is set to **Fault**. This error code is an HTTP error code.

Step 9 Click **OK**.

----End

Configuring Blacklist and Whitelist

Based on the public key authentication mechanism, ServiceComb engines provide the blacklist and whitelist functions. The blacklist and whitelist can be used to control which services can be accessed by microservices.

The blacklist and whitelist take effect only after public key authentication is enabled. For details, see **Configuring Public Key Authentication**.

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Microservice Governance**.

- For engines with security authentication disabled, go to **Step 6**.
- For engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

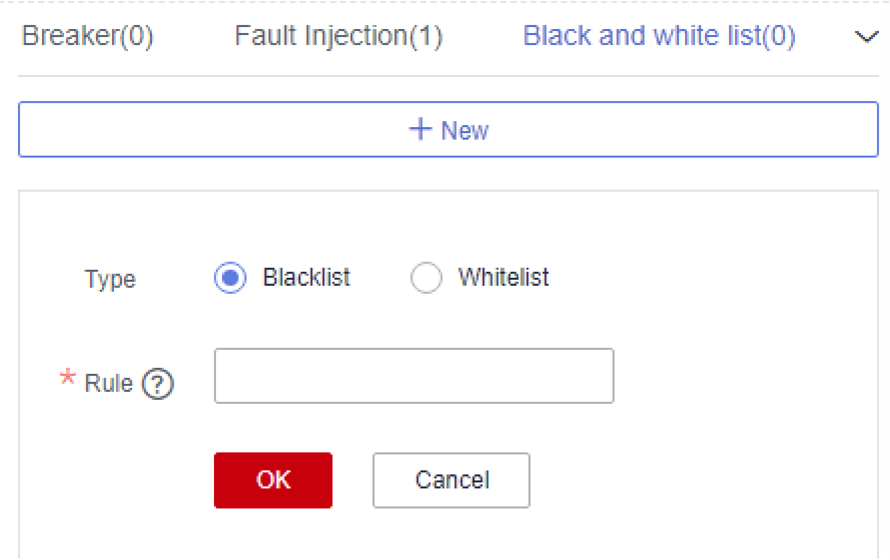
- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click the microservice to be governed.

Step 7 Click **Black and white list**.

Step 8 Click **New** to add a blacklist or whitelist for the application. The following table describes configuration items of blacklist and whitelist.

Figure 3-13 Configuring blacklist and whitelist



Configuration Item	Description
Type	- **Blacklist**: Microservices that match the matching rule are not allowed to access the current service. - **Whitelist**: Microservices that match the matching rule are allowed to access the current service.
Rule	Use a regular expression. For example, if **Rule** is set to **data***, services whose names start with **data** in the blacklist are not allowed to access the current service, or services whose names start with **data** in the whitelist are allowed to access the current service.

Step 9 Click **OK**.

----End

Configuring Public Key Authentication

Public key authentication is a simple and efficient authentication mechanism between microservices provided by CSE. Its security is based on the reliable interaction between microservices and the service center. That is, the authentication mechanism must be enabled between microservices and the service center. The procedure is as follows:

1. When the microservice starts, a key pair is generated and the public key is registered with the service center.
2. Before accessing the provider, the consumer uses its own private key to sign a message.
3. The provider obtains the public key of the consumer from the service center and verifies the signed message.

To enable public key authentication, perform the following steps:

1. Enable public key authentication for both the consumer and provider.
```
servicecomb:
  handler:
    chain:
      Consumer:
        default: auth-consumer
      Provider:
        default: auth-provider
```
2. Add the following dependency to the **pom.xml** file:
```
<dependency>
    <groupId>org.apache.servicecomb</groupId>
    <artifactId>handler-publickey-auth</artifactId>
  </dependency>
```

3.3.5 Configuration Management (Applicable to Engine 2.x)

ServiceComb engines define a configuration mechanism that is irrelevant to development frameworks. A configuration item consists of a key, label, and value. The label is used to identify whether a configuration item belongs to global configuration or microservice configuration. The label can also indicate the value type.

NOTICE

Configuration items are stored in plaintext. Do not include sensitive data.

You can refer to the following table to select the operations to be performed.

Operation	Description
Creating an Application-Level Configuration	Associates the new configuration with an application, and adds the application name and environment label.
Creating a Microservice-Level Configuration	Associates the new configuration with a microservice, and adds the microservice name, application name, and environment.
Creating a Customized Configuration Item	If application-level and microservice-level configurations cannot meet service requirements, you can customize configuration files.

Operation	Description
Importing Configurations	Imports the local configuration file.
Exporting Configurations	Exports the selected configuration file to the local host.
Comparing Configuration Versions	Compares differences between historical versions.
Rolling Back a Version	Rolls back to the selected historical version.
Viewing Historical Versions	Displays configurations of different historical versions.
Editing a Configuration Item	Edits a configuration item.
Disabling a Configuration Item	Disables a configuration item.
Deleting a Configuration Item	Deletes a configuration item.

NOTE

When the configuration item quota specified by the engine specifications is about to be used up, the engine allows new configuration items that exceed the remaining quota to be created to ensure capacity availability. Expand the capacity of the engine as soon as possible to prevent configuration creation failures.

Creating an Application-Level Configuration

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Configuration Management**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **Create Configuration Item** and set parameters by referring to the following table. Parameters marked with an asterisk (*) are mandatory.

Parameter	Description
*Configuration Item	Enter a configuration item. The configuration item is the global ID of the configuration. In the coding phase, the configuration item is used to index and operate the configuration. You are advised to use the Java package naming rule (for example, **cse.service.registry.address**) to ensure the readability and uniqueness of the configuration. **NOTE** Configuration items starting with **servicecomb.matchGroup.** cannot be created during application-level configuration creation. Such configuration items conflict with the configuration generated during service scenario governance creation, so the service scenario cannot be displayed.
Configuration Range	Select **Application-level**.
*Application	1. Select or enter an application name. 2. Select an environment.
Configuration Format	Select a configuration format. Common configuration formats such as TEXT, YAML, JSON, Properties, INI and XML can be edited online. The default value is **TEXT**.
*Configuration Content	Enter the configuration content.
Enable Configuration	Determine whether to enable the configuration item. ● **Enable now**: The configuration item takes effect immediately once created. ● **Not Enabled**: The configuration item does not take effect.

Step 7 Click **Create Now** to enable the configuration item.

----End

Creating a Microservice-Level Configuration

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Configuration Management**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **Create Configuration Item** and set parameters by referring to the following table. Parameters marked with an asterisk (*) are mandatory.

Parameter	Description
*Configuration Item	Enter a configuration item. The configuration item is the global ID of the configuration. In the coding phase, the configuration item is used to index and operate the configuration. You are advised to use the Java package naming rule (for example, **cse.service.registry.address**) to ensure the readability and uniqueness of the configuration.
Configuration Range	Select **Microservice-level**.
*Microservice	1. Select or enter a microservice name. 2. Select or enter an application name. 3. Select an environment.
Configuration Format	Select a configuration format. Common configuration formats such as TEXT, YAML, JSON, Properties, INI and XML can be edited online. The default value is **TEXT**.
*Configuration Content	Enter the configuration content.
Enable Configuration	Determine whether to enable the configuration item. ● **Enable now**: The configuration item takes effect immediately once created. ● **Not Enabled**: The configuration item does not take effect.

Step 7 Click **Create Now** to enable the configuration item.

----End

Creating a Customized Configuration Item

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Configuration Management**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **Create Configuration Item** and set parameters by referring to the following table. Parameters marked with an asterisk (*) are mandatory.

Parameter	Description
*Configuration Item	Enter a configuration item. The configuration item is the global ID of the configuration. In the coding phase, the configuration item is used to index and operate the configuration. You are advised to use the Java package naming rule (for example, **cse.service.registry.address**) to ensure the readability and uniqueness of the configuration.
Configuration Range	Select **Customize**.
*Labels	If application-level and microservice-level configurations cannot meet service requirements, you can use labels to customize configurations.
Configuration Format	Select a configuration format. Common configuration formats such as TEXT, YAML, JSON, Properties, INI and XML can be edited online. The default value is **TEXT**.
*Configuration Content	Enter the configuration content.

Parameter	Description
Enable Configuration	Determine whether to enable the configuration item. ● **Enable now**: The configuration item takes effect immediately once created. ● **Not Enabled**: The configuration item does not take effect.

Step 7 Click **Create Now** to enable the configuration item.

----End

Importing Configurations

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Configuration Management**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **Import** in the upper right corner to Import files in different formats as required, and set parameters by referring to the following table.

Table 3-6 V2.0 file

Parameter	Description
File Format	Select a format of the file to be imported. The default format is **V2.0**.
Import to Specific Environment	● Disabled: The imported configuration does not change the environment label. ● Enabled: Importing the configuration to a specific environment will change the environment label. Select an environment from the drop-down list.

Parameter	Description
Same Configuration	- **Terminate**: If a configuration is the same as that in the system, the import terminates. - **Skip**: During import, if a configuration is the same as that in the system, the configuration is skipped and other configurations are imported. - **Overwrite**: During import, if a configuration is the same as that in the system, the value of the configuration will be replaced.
Configuration File	Click **Import** and select the target file. **NOTE** The file size cannot exceed 2 MB.

Table 3-7 V1.0 file

Parameter	Description
File Format	Select **V1.0**.
*Import to Specific Environment	Select a microservice environment.
Microservice	Select the microservice to which the configuration is imported from the drop-down list.
Microservice Version	Select a version of the microservice to which the configuration is imported from the drop-down list.
*Configuration File	Click **Import** and select the target file. **NOTE** The file size cannot exceed 2 MB.

Step 7 Click **Close**.

----End

Exporting Configurations

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Configuration Management**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Select the configuration items to be exported and click **Export**.

- Click **Export** above the configuration items. In the displayed dialog box, click **Export**.
- Click **Export** in the upper right corner. In the displayed dialog box, select the file format (V2.0 by default) and click **OK**.

  NOTE

  If the format of the exported configuration file is V1.0, you need to select the microservice environment, microservice name, and microservice version from the drop-down list.

----End

Comparing Configuration Versions

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Configuration Management**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click the configuration item to be compared.

Step 7 Click **View Historical Version**.

Step 8 In **Historical Versions** on the left, select the historical version to be viewed.

In the **Configuration file** on the right, you can view the differences between the current and historical versions.

NOTE

A maximum of 100 historical versions can be displayed.

----End

Rolling Back a Version

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Configuration Management**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click the target configuration item.

Step 7 Click **View Historical Version**.

Step 8 In **Historical Versions** on the left, select the target historical version.

Step 9 In **Configuration file** on the right, click **Roll Back to the Selected Version**.

----End

Viewing Historical Versions

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Configuration Management**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **View Historical Version** in the **Operation** column of a configuration item. On the **Historical Versions** page that is displayed, you can view the historical versions of the configuration item. On this page, you can compare the configuration version with the rollback version.

----End

Editing a Configuration Item

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Configuration Management**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **Edit** in the **Operation** column of the target configuration item. You can also click the target configuration item and then click **Edit** on the displayed configuration details page.

Step 7 Enter the configuration information in the **Configuration Content** text box and click **Save**.

----End

Disabling a Configuration Item

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Configuration Management**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 In the **Operation** column of the target configuration item, click **More** > **Disable**.

Step 7 Click **OK**.

----End

Deleting a Configuration Item

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Configuration Management**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **Delete** in the **Operation** column of the target configuration item. You can also click the target configuration item and then click **Delete** on the displayed configuration details page.

Step 7 Click **OK**.

----End

3.3.6 Configuration Management (Applicable to Engine 1.x)

The configuration added here is a global configuration. After being added, the configuration takes effect immediately if all microservices registered with the engine use it.

If dynamic configuration is set for a single microservice, the dynamic configuration overwrites the global configuration. For details about how to set dynamic configuration, see **Dynamic Configuration**.

Creating a Configuration

Configuration management provides common configurations for microservices, such as log levels and running parameters. After being added, the configuration item is used as the default one if no same configuration items are defined for microservices.

NOTICE

Configuration items are stored in plaintext. Do not include sensitive data.

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Configuration Management**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **Create Configuration Item**.

Step 7 On the **Create Configuration Item** page, select a microservice environment and enter **Configuration Item** and **Value**.

Step 8 Click **OK**.

----End

Importing Configurations

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Configuration Management**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **Import**.

Step 7 Select a microservice environment, click **Import**, and select the target file.

NOTE

A maximum of 150 configuration items can be imported at a time.

Step 8 Click **Close**.

----End

Exporting Configurations

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Configuration Management**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **Export All**.

----End

Deleting a Configuration

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Configuration Management**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Select the target configuration item and click **Delete**. You can also click **Delete** in the **Operation** column of the target configuration item.

Step 7 Click **OK**.

----End

Editing a Configuration

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target engine.

Step 4 Choose **Configuration Management**.

- For ServiceComb engines with security authentication disabled, go to **Step 6**.
- For ServiceComb engines with security authentication enabled, go to **Step 5**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click **Edit** in the **Operation** column of the target configuration item and edit the values of the configuration item.

Step 7 Click **OK**.

----End

3.3.7 System Management

3.3.7.1 Overview

A ServiceComb engine may be used by multiple users. Different users must have different ServiceComb engine access and operation permissions based on their responsibilities and permissions.

The exclusive ServiceComb engine with security authentication enabled provides the system management function using the role-based access control (RBAC) through the microservice console.

The exclusive ServiceComb engine with security authentication enabled supports the access of Spring Cloud and Java chassis microservice frameworks.

NOTE

- The RBAC-based system management function is irrelevant to IAM permission management. It is only an internal permission management mechanism of CSE.
- To operate a ServiceComb engine on CSE, you must have both the IAM and RBAC permissions, and the IAM permission takes precedence over the RBAC permission.
- If you perform operations on a ServiceComb engine through APIs or the microservice framework, you only need to have the RBAC permissions.

1. You can use an account associated with the **admin** role to create an account and associate a proper role with the account based on service requirements. The user who uses this account has the access and operation permissions on the ServiceComb engine.
   - When you create an exclusive ServiceComb engine with security authentication enabled, the system automatically creates the **root** account associated with the **admin** role. The **root** account cannot be edited or deleted.
   - You can create an account using the **root** account of the ServiceComb engine or an account associated with the **admin** role of the ServiceComb engine. For details about how to create and manage an account, see **Accounts**.

2. You can create a custom role using an account associated with the **admin** role and grant proper ServiceComb engine access and operation permissions to the role based on service requirements.
   - The system provides two default roles: administrator (**admin**) and developer (**developer**). Default roles cannot be edited or deleted.
   - You can create a custom role using the **root** account of the ServiceComb engine or an account associated with the **admin** role of the ServiceComb engine. For details about how to create and manage a role, see **Roles**.
   - For details about role permissions, see **Table 3-8**.

Table 3-8 Role permissions

Role	Permission Description
Admin	Full permissions for all microservices, accounts, and roles of the ServiceComb engine.
Developer	Full permissions for all microservices of the ServiceComb engine.
Custom role	You can create roles based on service requirements and grant microservice operation and configuration permissions to the roles.

3.3.7.2 Accounts

You can use an account associated with the **admin** role to log in to the ServiceComb engine console and create an account or manage a specified account created in the engine based on service requirements.

Table 3-9 Account management operations

Operation	Description
Adding an Account	Creates an account and associates a proper role with the account. Users who use the account have the access and operation permissions on the ServiceComb engine. You can create up to 1000 accounts, including new accounts and imported IAM account.

Operation	Description
Importing an IAM Account	Imports an IAM account and associates roles with it. Users using this IAM account have the access and operation permissions on the microservice engine. If the imported IAM account needs to connect microservice applications to the engine through programming interface authentication, **reset** its password and then use the new password to configure security authentication parameters. When you use this IAM account to log in to the CSE console with security authentication enabled, you do not need to enter the account and password. However, a password is still required after the VDC read-only user is imported. CSE can manage up to 1000 accounts, including new accounts and imported IAM account. **NOTE** The IAM account can be imported only to ServiceComb engine 2.5.0 or later with security authentication enabled.
Viewing Role Permissions	Displays the permissions of the role associated with a specified account.
Editing an Account	Adds or deletes roles for an account. The **root** account cannot be edited.
Changing the Password	Changes the password of an account that has logged in to the ServiceComb engine based on service requirements or security regulations. **NOTICE** ● If the account and password are used to register a microservice in the SDK, changing the account and password may affect the service running of the microservice (the microservice cannot be registered with the ServiceComb engine). As a result, the service system will be damaged. Exercise caution when performing this operation. ● After the password is changed, update the microservice authentication configuration in a timely manner. ● Spring Cloud: see **Connecting Spring Cloud Applications to ServiceComb Engines**. ● Java Chassis: see **Connecting Java Chassis Applications to ServiceComb Engines**. ● After the password is changed, the account may be locked due to three consecutive incorrect password attempts. The account will be unlocked after 15 minutes.

Operation	Description
Resetting a Password	Based on service requirements or security regulations, you can use the account that has logged in to the ServiceComb engine to reset the passwords of other accounts under the ServiceComb engine. **NOTICE** ● If the account and password are used to register a microservice in the SDK, resetting the account and password may affect the service running of the microservice (the microservice cannot be registered with the ServiceComb engine). As a result, the service system will be damaged. Exercise caution when performing this operation. ● After the password is reset, update the microservice authentication configuration in a timely manner. ● Spring Cloud: see **Connecting Spring Cloud Applications to ServiceComb Engines**. ● Java Chassis: see **Connecting Java Chassis Applications to ServiceComb Engines**. ● After the password is reset, the account may be locked due to three consecutive incorrect password attempts. The account will be unlocked after 15 minutes.
Deleting an Account	Deletes an account that is no longer used. The **root** account cannot be deleted. **NOTICE** If the account and password are used to register a service in the SDK, deleting the account will affect the service running (the account cannot be registered with the engine) and damage the service system. Exercise caution when performing this operation.

Adding an Account

Before adding an account, you can create a role based on service requirements. For details, see **Creating a Role**.

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target ServiceComb engine with security authentication enabled.

Step 4 Choose **System Management**.

Step 5 In the displayed **Security Authentication** dialog box, enter the name and password of the account associated with the **admin** role under the ServiceComb engine, and click **OK**.

NOTE

If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.

Step 6 Choose **Accounts** > **Create Account** and configure account parameters by referring to the following table:

Parameter	Description
Account	Enter an account name. **NOTE** The account name cannot be changed once the account is created.
Role	Select a role based on service requirements. **NOTE** An account can be associated with up to five roles.
Password	Enter the password.
Confirm Password	Enter the password again.

Step 7 Click **OK**.

----End

Importing an IAM Account

Before importing an IAM account, you can create a role based on service requirements. For details, see **Creating a Role**.

Step 1 **Log in to CSE**.

Step 2 Click the target ServiceComb engine with security authentication enabled.

Step 3 Choose **System Management**. In the displayed **Security Authentication** dialog box, enter the name and password of the account associated with the **admin** role under the ServiceComb engine, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 4 Choose **Accounts** > **Import IAM User Name**.

Step 5 Select the IAM account to be imported and select account roles.

NOTE

An account can be associated with up to five roles.

Step 6 Click **Confirm**.

NOTE

You cannot use the passwords of the imported IAM user names to log in to the system. **Resetting a Password** first if you want to use the imported IAM user names to connect microservice applications to the engine through programming interface security authentication.

----End

Viewing Role Permissions

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target ServiceComb engine with security authentication enabled.

Step 4 Choose **System Management**.

Step 5 In the displayed **Security Authentication** dialog box, enter the name and password of the account associated with the **admin** role under the ServiceComb engine, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 Click the role in the **Role** column of the account to be viewed in the account list. On the displayed page, view the role and permission configuration associated with the account.

----End

Editing an Account

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target ServiceComb engine with security authentication enabled.

Step 4 Choose **System Management**.

Step 5 In the displayed **Security Authentication** dialog box, enter the name and password of the account associated with the **admin** role under the ServiceComb engine, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 On the **Accounts** tab page, click **Edit Account** in the **Operation** column of the account to be edited.

Step 7 Select a role based on service requirements.

NOTE

An account can be associated with up to five roles.

Step 8 Click **Save**.

----End

Changing the Password

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target ServiceComb engine with security authentication enabled.

Step 4 Choose **System Management**.

Step 5 In the displayed **Security Authentication** dialog box, enter the account name and password, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**
- The account for connecting to the ServiceComb engine is not associated with the admin role. You can only change the password of the current login account.
- The account for connecting to the engine is associated with the admin role. You can change the passwords of all accounts of the ServiceComb engine.
- For details about how to create an account, see **Adding an Account**.

Step 6 On the **Accounts** tab, select the account for logging in to the ServiceComb engine and click **Reset Own Password** in the **Operation** column.

1. Enter the old password and a new password, and confirm the password.
2. After confirming that the password needs to be changed, select **I Understand**.

NOTE

You can also click **Reset Own Password** in the upper right corner of the **System Management** page to change the password of the current login account.

Step 7 Click **Save**.

----End

Resetting a Password

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target ServiceComb engine with security authentication enabled.

Step 4 Choose **System Management**.

Step 5 In the displayed **Security Authentication** dialog box, enter the name and password of the account associated with the **admin** role under the ServiceComb engine, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 On the **Accounts** tab page, select the account whose password is to be reset, and click **Reset Password** in the **Operation** column.

1. Enter a new password and confirm the password.
2. After confirming that the password needs to be reset, select **I Understand**.

Step 7 Click **Save**.

----End

Deleting an Account

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target ServiceComb engine with security authentication enabled.

Step 4 Choose **System Management**.

Step 5 In the displayed **Security Authentication** dialog box, enter the name and password of the account associated with the **admin** role under the ServiceComb engine, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 On the **Accounts** tab page, click **Delete** in the **Operation** column of the account to be deleted.

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

----End

3.3.7.3 Roles

In addition to the default roles **admin** and **developer**, you can use a ServiceComb engine account associated with the **admin** role to log in to the CSE console and perform operations listed in **Table 3-10** based on service requirements.

Table 3-10 Role management operations

Operation	Description
Creating a Role	Creates a role and configures permission actions for the role in different service and configuration groups. A maximum of 100 roles can be created.
Editing a Role	Modifies the permissions of the created role.

Operation	Description
Deleting a Role	Deletes a role that is no longer used. **NOTE** ● Deleted roles cannot be restored. Exercise caution when performing this operation. ● Before deleting a role, ensure that the role is not associated with any account. For details about how to cancel the association between a role and an account, see **Editing an Account**.
Viewing a Role	Displays the created roles of the ServiceComb engine based on the keyword of the role name.

Creating a Role

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target ServiceComb engine with security authentication enabled.

Step 4 Choose **System Management**.

Step 5 In the displayed **Security Authentication** dialog box, enter the name and password of the account associated with the **admin** role under the ServiceComb engine, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 On the **Roles** tab page, click **Create Role**.

Step 7 Enter a role name.

NOTE

The role name cannot be changed once the role is created.

Step 8 Configure permissions.

1. Set **Permission Group**.
   a. Set the service permissions.
      - If you select **All Services**:

        You can perform corresponding permission actions on all microservices of the ServiceComb engine.
      - If you select **Custom Service Groups**, set the parameters according to **Table 3-11**.

Table 3-11 Custom service group operations

Operation	Description
Adding a Matching Rule	Click **Add Service Group Matching Rule**. Select **Application**, **Environment**, and **Service** based on service requirements to filter the microservices on which the role can perform permission actions. **NOTE** **Application**, **Environment**, and **Service** are three parameters of a microservice: ○ If only one parameter is set for a single matching rule, the role has the operation permission on the microservice that matches the parameter value. For example, if you add **Environment: production**, the role has the operation permission only on the microservice whose environment name is **production**. ○ If more than one parameter is set for a single matching rule, the role has the operation permission on the microservices that match all parameter values. For example, if you add **Environment: production Application: abc**, the role has the operation permission on the microservice whose environment name is **production** and application name is **abc**. ○ When automatic discovery is enabled, microservices query the instance addresses of services such as the registry center, configuration center, and dashboard through the registry center. When you grant the query permission to a microservice, the permission of the default application must be included. In this case, add the matching rule **Application: default**. After the microservice matching rule is set, click **OK**.
Editing a Matching Rule	Click ✎ next to the matching rule to be edited. You can reconfigure **Service Group** and **Action** of the matching rule based on service requirements. After the service group matching rule is set, click **OK**.
Deleting a Matching Rule	Click 🗑 next to the matching rule to be deleted. You can delete the matching rule based on service requirements.

NOTE

A maximum of 20 microservice matching rules can be set for a custom service group.

If multiple matching rules are set for a custom service group, the role has the operation permission on the microservice as long as the microservice meets any of the matching rules.

b. Set the configuration permissions.

- If you select **All Configurations**:

  You can perform corresponding permission actions on all microservices of the ServiceComb engine.

- If you select **Custom Configuration Groups**, set the parameters according to **Table 3-12**.

Table 3-12 Custom configuration group operations

Operation	Description
Adding a Matching Rule	Click **Add Configuration Group Matching Rule**. Select **Application**, **Environment**, and **Service** based on service requirements to filter the configurations on which the role can perform permission actions. If application-level and microservice-level configurations cannot meet service requirements, you can customize a matching rule to match the configured custom labels and filter the permission actions that can be performed by the role. **NOTE** **Application**, **Environment**, and **Service** are three parameters of a configuration: ○ If only one parameter is set for a single matching rule, the role has the operation permission on the configuration that matches the parameter value. For example, if you add **Environment: production**, the role has the operation permission only on the configuration whose environment name is **production**. ○ If more than one parameter is set for a single matching rule, the role has the operation permission on the configurations that match all parameter values. For example, if you add **Environment: production Application: abc**, the role has the operation permission on the configuration whose environment name is **production** and application name is **abc**. After the configuration matching rule is set, click **OK**.
Editing a Matching Rule	Click ✎ next to the matching rule to be edited. You can reconfigure **Configuration Group** and **Action** of the matching rule based on service requirements. After the configuration group matching rule is set, click **OK**.
Deleting a Matching Rule	Click 🗑 next to the matching rule to be deleted. You can delete the matching rule based on service requirements.

> **NOTE**
>
> A maximum of 20 matching rules can be set for a custom configuration group.
>
> If multiple matching rules are set for a configuration service group, the role has the operation permission on the configuration as long as the configuration meets any of the matching rules.

2. Set **Action**.

   Configure the permission actions that can be performed by the role on the selected service group and configuration group based on service requirements. You can select multiple permission actions.

   - **All**: Add, delete, modify, and query resources in the service group and configuration group.
   - **Add**: Add resources to the service group and configuration group.
   - **Delete**: Delete resources from the service group and configuration group.

     > **NOTE**
     >
     > If only **Delete** is selected, you cannot delete resources in the service group and configuration group. You must select **View** at the same time.

   - **Modify**: Modify resources in the service group.

     > **NOTE**
     >
     > If only **Modify** is selected, you cannot modify resources in the service group and configuration group. You must select **View** at the same time.

   - **View**: View resources in the service group and configuration group.

Step 9 Click **Create**.

----End

Editing a Role

Step 1 **Log in to CSE**.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target ServiceComb engine with security authentication enabled.

Step 4 Choose **System Management**.

Step 5 In the displayed **Security Authentication** dialog box, enter the name and password of the account associated with the **admin** role under the ServiceComb engine, and click **OK**.

> **NOTE**
>
> - If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
> - For details about how to create an account, see **Adding an Account**.

Step 6 On the **Roles** tab page, click **Edit** in the **Operation** column of the role to be edited.

Step 7 Modify **Service Group**, **Configuration Group**, and **Action** based on service requirements.

Step 8 Click **Save**.

----End

Deleting a Role

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target ServiceComb engine with security authentication enabled.

Step 4 Choose **System Management**.

Step 5 In the displayed **Security Authentication** dialog box, enter the name and password of the account associated with the **admin** role under the ServiceComb engine, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 On the **Roles** tab page, click **Delete** in the **Operation** column of the role to be deleted. In the displayed dialog box, enter **DELETE** and click **OK**.

NOTE

- Deleted roles cannot be restored. Exercise caution when performing this operation.
- Before deleting a role, ensure that the role is not associated with any account. For details about how to cancel the association between a role and an account, see **Editing an Account**.

----End

Viewing a Role

Step 1 Log in to CSE.

Step 2 Choose **Exclusive ServiceComb Engines**.

Step 3 Click the target ServiceComb engine with security authentication enabled.

Step 4 Choose **System Management**.

Step 5 In the displayed **Security Authentication** dialog box, enter the name and password of the account associated with the **admin** role under the ServiceComb engine, and click **OK**.

NOTE

- If you connect to the ServiceComb engine for the first time, enter the account name **root** and the password entered when **Creating a ServiceComb Engine**.
- For details about how to create an account, see **Adding an Account**.

Step 6 On the **Roles** tab page, click ⌄ next to the role to be viewed to expand the role details.

Service Group, **Configuration Group**, and **Action** of the role are displayed.

----End

4 Registry/Configuration Center

4.1 Creating a Registry/Configuration Center

This section describes how to create an engine whose registry/configuration center is Nacos.

NOTE

Nacos engines are supported only in CN East 2, CN-Hong Kong, AP-Singapore, ME-Riyadh, and LA-Mexico City2.

Prerequisites

- A Nacos engine runs on a VPC. Before creating a Nacos engine, ensure that VPCs and subnets are available. For details about how to create a VPC and subnet, see **Creating a VPC**.
- The user has the CSE FullAccess and DNS Full Access permissions.

Creating a Registry/Configuration Center

Step 1 Go to **Buy Registry/Configuration Center Instance**.

Step 2 Set parameters according to the following table. Parameters marked with an asterisk (*) are mandatory.

Parameter	Description
*Billing Mode	Billing mode. Currently, **Pay-per-use** is supported.
*Enterprise Project	Project where the Nacos engine locates. You can search for and select an enterprise project in the drop-down list. Enterprise projects let you manage cloud resources and users by project. An enterprise project can be used after it is created and enabled. For details, see **Enabling the Enterprise Project Function**. By default, **default** is selected.

Parameter	Description
*Name	Name of a Nacos engine. The name contains 3 to 64 characters, including letters, digits, and hyphens (-), and starts with a letter but cannot end with a hyphen. **NOTICE** Nacos engine name cannot be **default**.
*Registry/ Configuration Center Instance	Select **Nacos**. **NOTE** Cluster nodes in the registry/configuration center are evenly distributed to different AZs. A failure of a single node does not affect external services. The registry/configuration center does not support AZ-level DR but provides host-level DR.
*Instances	Select the required capacity specifications. **NOTE** To create a Nacos engine with more than 2,000 microservice instances, submit a **service ticket**.
Version	Only the latest version can be created.
*Network	Select a VPC and subnet to provision logically isolated, configurable, and manageable virtual networks for your engine. ● To use a created VPC, search for and select a VPC created under the current account from the drop-down list. ● To use a new VPC, click **console** to go to the **Virtual Private Cloud** page and create one. For details, see **Creating a VPC**. **NOTE** ● You cannot use a shared VPC to create a Nacos engine. Otherwise, the engine fails to be created. ● The VPC cannot be changed once the Nacos engine is created.
Tag	Tags are used to identify cloud resources. When you have multiple cloud resources of the same type, you can use tags to classify them based on usage, owner, or environment. Click ⊕ **Add Tag**. In the **Add Tag** dialog box, enter a tag key and value. For details about tag naming rules, see **Managing Tags**. In the **Add Tag** dialog box, you can click ⊕ **Add Tag** to add multiple tags at a time, or click ⊖ next to a tag to delete the tag.

Step 3 Click **Buy**. The page for confirming the engine information is displayed.

Step 4 Click **Submit**. When the status becomes **Available**, the engine is created.

NOTE

- After the Nacos engine is created, its status is **Available**. For details about how to view the Nacos engine status, see **Viewing Nacos Engine Information**.
- You may fail in buying an engine for insufficient underlying resources. To prevent this, delete engines in time so that you will not be charged if your engines restore upon sufficient underlying resources.

----End

4.2 Managing a Registry/Configuration Center

4.2.1 Viewing Nacos Engine Information

This section describes how to view details about a Nacos instance on the CSE console.

Viewing Nacos Engine Information

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

NOTE

You can click an **Available** instance to go to the **Basic Information** page.

Step 4 View the Nacos engine information shown in **Table 4-1**.

Table 4-1 Engine details

Type	Parameter	Description
Basic Information	Name	Engine name entered when **Creating a Registry/Configuration Center**. Click ⧉ to copy it. An engine name can be changed. The name contains 3 to 64 characters, including letters, digits, and hyphens (-), and starts with a letter but cannot end with a hyphen.
	ID	Engine ID. Click ⧉ to copy it.
	Running Status	Engine status.
	Registry/Configuration Center Instance	Select **Nacos**.
	Version	Engine version.
	Capacity Specifications	Engine specifications selected when **Creating a Registry/Configuration Center**. If the engine is a small-scale engine, click **Change Specifications** on the right to expand the capacity. For details, see **Increasing Nacos Engines**.

Type	Parameter	Description
	Enterprise Project	Enterprise project selected when **Creating a Registry/ Configuration Center**.
	Billing Mode	Billing mode selected in **Creating a Registry/Configuration Center**. Only pay-per-use billing is supported.
	Created	Time when **Creating a Registry/Configuration Center**.
Connection Information	Private IP	Internal IP address of a Nacos engine.
	Private Port	Internal port of a Nacos engine.
	Virtual Private Cloud	VPC selected when you **create a registry/configuration center**.
	Subnet	Subnet selected when you **create a registry/configuration center**.
	Whitelist Access	Nacos supports whitelist control. Multiple IP addresses or IP address segments can be configured. IP addresses that are not in the IP address segments cannot be accessed. For details about whitelist access, see **Managing the Nacos Engine Whitelist**.
More Settings	Tag	Tags added to the Nacos engine. You can also click **Tag Management** and perform operations on tags as required. For details, see **Managing Tags**.

----End

4.2.2 Increasing Nacos Engines

You can increase the number of Nacos engines online. Only low-capacity engines support this operation.

Increasing Nacos Engines

Step 1 **Log in to CSE**.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click **More** > **Change Specifications** in the **Operation** column of the target Nacos engine instance. Alternatively, click the target engine and click **Change Specifications** next to **Capacity Specifications** in the **Basic Information** area on the **Basic Information** page.

Step 4 On the **Change Nacos Engine Specifications** page, select the target capacity.

Step 5 Click **Change Now**, confirm the information, and click **Submit**. When the instance status changes from **Changing** to **Available**, the operation is successful.

----End

4.2.3 Deleting a Nacos Engine

You can delete a Nacos engine if it is no longer used.

NOTICE

Deleted engines cannot be recovered. Exercise caution when performing this operation.

Background

You can delete Nacos engines in the following states:

- Available
- Unavailable
- Creation failed
- Resizing failed
- Upgrade failed

Deleting a Nacos Engine

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click **More** > **Delete** in the **Operation** column of the target Nacos engine instance. Alternatively, click the target Nacos engine, click **Delete** in the upper right corner on the **Basic Information** page, and enter **DELETE** and click **OK** in the displayed dialog box.

NOTE

If the deletion fails, click **Force Delete**.

----End

4.2.4 Upgrading a Nacos Engine

Nacos engines are created using the latest engine version. When a later version is released, you can upgrade your engine.

NOTE

- During the Nacos engine upgrade, the microservice and engine are intermittently disconnected, but services of running microservices are not affected. You are advised not to upgrade, restart, or change microservices when upgrading a Nacos engine.
- Version rollback is not supported after the upgrade.
- You can only upgrade to the latest version.

Upgrading a Nacos Engine

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click ↑ in the **Version** column of the target Nacos engine.

> **NOTE**
>
> If the engine version is the latest, ↑ does not exist in the **Version** column.

Step 4 In the displayed dialog box, confirm the current and target versions, and click **OK**.

If the upgrade fails, click **Retry** to perform the upgrade again.

----End

4.2.5 Managing Tags

Tags facilitate Nacos engine identification and management.

If your organization has configured tag policies for Nacos engines, add tags to engines based on the policies. If a tag does not comply with the tag policies, engine creation may fail. Contact your administrator to learn more about tag policies.

You can add tags to a Nacos engine when creating the engine or add tags on the details page of the created engine. Up to 20 tags can be added to an engine. Tags can be modified and deleted.

A tag consists of a tag key and a tag value. **Table 4-2** lists the tag key and value requirements.

Table 4-2 Tag naming rules

Tag	Rule
Key	• Cannot be left blank. • Must be unique for the same instance. • Contain a maximum of 128 characters. • Contain only letters, digits, spaces, and special characters (_ . : = + - @). • Cannot start with a space or **_sys_** or end with a space.
Value	• Contain a maximum of 255 characters. • Contain only letters, digits, spaces, and special characters (_ . : = + - @).

Managing Tags

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target engine. The details page is displayed.

Step 4 In the **More Settings** area, perform the following operations in the **Tags** field as required:

- Add a tag

  NOTICE

  Adding tags will affect Nacos engine services for about 10 seconds. Add tags during off-peak hours.

  a. Click **Tag Management**. The **Edit Tag** dialog box is displayed.

  b. Click ⊕ **Add Tag** and enter a tag key and value in the text boxes.

  c. Click **OK**.

- Modify a tag

  NOTICE

  Modifying tags will affect Nacos engine services for about 10 seconds. Modify tags during off-peak hours.

  a. Click **Tag Management**. The **Edit Tag** dialog box is displayed.

  b. You can modify the tag key and value in the original text boxes.

  c. Click **OK**.

- Delete a tag

  Click ⊖ in the row that contains the tag to be deleted. In the dialog box that is displayed, click **OK** to delete the tag.

----End

4.2.6 Modifying the Maintenance Time Window of a Nacos Engine

You can modify the maintenance time window of a Nacos engine on the instance's details page of the console. During the maintenance time window, O&M personnel can maintain the instance.

Prerequisites

A Nacos engine has been created.

Modifying the Maintenance Time Window of a Nacos Engine

Step 1 **Log in to CSE**.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the Nacos engine to be modified.

Step 4 On the Nacos engine details page, click ✎ next to **Maintenance Window**.

Step 5 Select a new maintenance window from the drop-down list. Click ✓ to save the modification or ✕ to discard the modification.

The modification will take effect immediately on the **Basic Information** tab page.

NOTE

The duration of each maintenance window is one hour, for example, from 02:00 to 03:00.

----End

4.2.7 Managing the Nacos Engine Whitelist

The following describes how to manage whitelists of a Nacos engine to allow access only from whitelisted IP addresses.

If no whitelists are added to the engine whitelist or the whitelist function is disabled, all IP addresses that can communicate with the VPC can access the engine.

NOTE

The owner of a shared VPC can add the VPC subnet to the whitelist to allow other tenants in the VPC to access the engine.

Setting a Whitelist

Step 1 **Log in to CSE**.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target engine. The details page is displayed.

NOTE

You can click an **Available** engine to go to the **Basic Information** page.

Step 4 In the **Connection Information** area, click ✎. In the **Set Access Whitelist** dialog box, enter **IP Address/Address Segment**. Use commas (,) to separate multiple whitelists.

NOTE

A maximum of 20 IP addresses/address segments can be added for each engine. IPv4 and IPv6 addresses are supported only in CN East 2. In other regions, only IPv4 addresses are supported.

- To modify or delete an IP address/address segment, modify or delete it in the displayed dialog box.

- To add an IP address/address segment, add it in the displayed dialog box.

Step 5 Click **OK**. When the engine status changes from **Configuring** to **Available**, the whitelist takes effect.

----End

4.3 Using a Registry/Configuration Center

4.3.1 Namespace Management

Namespaces isolate configurations in different environments. For example, resources (such as configurations and services) in the development and test environments are isolated from those in the production environment. Different namespaces can have the same group or data ID.

Precautions

- The namespace ID is entered in the SDK connected to a Nacos engine. The namespace name is only the identifier used for viewing on the console.
- If your service SDK uses a namespace ID that is not created on the Nacos server for service registration and discovery, the service can be registered and discovered, but cannot be viewed on the service management page of the registry/configuration center. You need to create the corresponding namespace before viewing the service. For details, see **Creating a Namespace**.

Prerequisites

You have created a Nacos engine instance. For details, see **Creating a Registry/Configuration Center**.

Creating a Namespace

NOTE

When an instance is created, a default namespace **public** (reserved space) is automatically generated. This namespace cannot be edited or deleted. You can use this namespace to isolate resources and services. Up to 50 namespaces can be created.

Step 1 **Log in to CSE**.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 Choose **Namespaces** and click **Create Namespace**.

Step 5 In the displayed dialog box, set the parameters as follows. Configuration items marked with an asterisk (*) are mandatory.

Table 4-3 Namespace parameters

Parameter	Description
*Namespace	The namespace name can be customized and can contain a maximum of 128 characters except @ # $% ^ & *.
Namespace ID	Enter a maximum of 128 characters. Use only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_). The namespace ID must be unique. **NOTE** If no ID is entered during creation, the system randomly generates an ID.

Step 6 Click **OK**.

----End

Editing a Namespace

Step 1 **Log in to CSE**.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 Choose **Namespaces**.

Step 5 Click **Edit** in the **Operation** column of the namespace to be edited to edit the namespace name.

NOTE

The automatically generated namespace **public** cannot be edited.

Step 6 Click **OK**.

----End

Deleting a Namespace

Step 1 **Log in to CSE**.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 Choose **Namespaces**.

Step 5 Click **Delete** in the **Operation** column of the namespace to be deleted.

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

----End

4.3.2 Service Management

You can use the CSE console to manage services registered with Nacos.

Prerequisites

A Nacos engine instance has been created.

Creating a Service

You can create a service on the console. The newly created service is an empty service (that is, the number of providers is 0). By default, the empty service is displayed in the service list. If you do not want to display the empty service, click ◯ next to **Hide Empty Service**.

Step 1 **Log in to CSE**.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 Choose **Service Management**.

Step 5 Select a namespace from the Namespace drop-down list. The ID is automatically filled in the Namespace ID box.

> NOTE
>
> If the selected namespace is **public**, the namespace ID is empty by default.

Step 6 Click **Create Service**. In the displayed dialog box, set configuration items as follows. Configuration items marked with an asterisk (*) are mandatory.

Table 4-4 Parameters

Parameter	Description
*Service Name	Enter a service name. The value can contain a maximum of 236 characters, including digits, letters, and special characters "_-.:".
Group	Set the group to which the service belongs. The value can contain a maximum of 128 characters, including digits, letters, and special characters "_-.:".
*Protection Threshold	If the ratio of healthy instances to the total instances is less than the threshold, a protection threshold is triggered. The value ranges from 0 to 1. The default value is **0**.

Step 7 Click **OK**.

----End

Viewing the Service List

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 Choose **Service Management**. Select a namespace from the **Namespace** drop-down list. The ID is automatically filled in the **Namespace ID** box.

NOTE

If the selected namespace is **public**, the namespace ID is empty by default.

Step 5 View all services in the namespace of the engine.

You can search for the target service by service name or group name.

NOTE

Target service fuzzy search supports characters: ,$*+.|?

----End

Viewing Service Details

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 Choose **Service Management**.

Step 5 Click the target service to view its details.

- View basic service information, including the service name, namespace name, service group, namespace ID, protection threshold, and number of clusters.
- The **Instances** tab displays the instance information, including the IP address, port number, cluster, health status, online/offline status, weight, and metadata. You can also perform **Instance Operations**, such as searching for instances based on metadata, bringing instances online/offline, and modifying weights.
- The **Subscribers** tab displays the list of all client instances that subscribe to the current service. Versions of subscribers and clients are displayed in the list.

----End

Instance Operations

- Search by metadata: On the **Instances** tab, select a cluster from **Clusters**, enter the metadata key and value in **Search Metadata**, and click **Filter** to display the instances that meet the search criteria. Click **Clear** to clear the search data.

- Bring an instance online or offline: On the **Instances** tab, click **Online** or **Offline** in the **Operation** column of the target instance. The instance status will be updated accordingly.
- Modify instance weight: On the **Instances** tab, move the cursor to the **Weight** column of the target instance, click ✎ to modify the weight (ranging from 1 to 99), and click **OK**.

  NOTE

  To use the Nacos weight function for traffic load balancing, register **NacosRule** provided by Nacos as a bean on the client.

  ```
  @Bean
  NacosRule nacosRule() {
     return new NacosRule();
  }
  ```

  Add the following configuration item to the **application.properties** configuration file:

  ```
  xxx-service.ribbon.NFLoadBalancerRuleClassName=com.alibaba.cloud.nacos.ribbon.NacosRule
  ```

  xxx-service indicates the service name of the client, that is,

  ```
  spring.application.name=xxx-service
  ```

Deleting a Service

NOTE

- Only empty services can be deleted. If the number of instance is not 0, the services cannot be deleted.
- If a service remains empty for more than 1 minute, the Nacos automatically deletes the service.

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 In the left navigation pane, choose **Service Management** and click **Delete** in the **Operation** column of the target service.

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

----End

4.3.3 Configuration Management

4.3.3.1 Creating a Configuration

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 In the left navigation pane, choose **Configuration Management** > **Configurations**.

Step 5 Select a namespace from the Namespace drop-down list. The ID is automatically filled in the Namespace ID box.

NOTE

If the selected namespace is **public**, the namespace ID is empty by default.

Step 6 Click **Create Configuration**. In the displayed dialog box, set the following parameters. Parameters marked with an asterisk (*) are mandatory.

Table 4-5 Parameters

Parameter	Description
*Data ID	The data ID is one of the dimensions for identifying configurations, and usually identifies configuration sets of a system. A system or application can contain multiple configuration sets, and each one can be identified by a name. A unique data ID is generally named like a Java package. This naming rule is optional. The value can contain a maximum of 255 characters, including digits, letters, and special characters "_-.:".
Group	It is a set of configurations in Nacos and one of the dimensions for identifying configurations. The value can contain a maximum of 128 characters, including digits, letters, and special characters "_-.:".
Namespace	Namespace to which the configuration belongs.
Configuration Format	Nacos supports online editing of common configuration formats such as YAML, Properties, TEXT, JSON, XML and HTML. The default value is **TEXT**.
*Configuration Content	Enter the configuration content. **NOTE** The configuration content cannot exceed 100 KB. If the configuration content is too large, split the configuration. Adjusting the configuration content size may affect Nacos stability. Exercise caution when performing this operation. To adjust the configuration content size, **submit a service ticket**.
Description	Enter the description. The value can contain a maximum of 128 characters.

Parameter	Description
Application	Enter the application to which the configuration belongs. The value can contain a maximum of 128 characters, including digits, letters, and special characters "_-.:".
Label	Enter a label. The value can contain a maximum of 64 characters, including digits, letters, and special characters "_-.:".

Step 7 Click **Release**.

----End

4.3.3.2 Querying Configurations

CSE Nacos allows you to query configurations by data ID, group, application, and label.

Step 1 **Log in to CSE**.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 In the left navigation pane, choose **Configuration Management** > **Configurations**.

Step 5 In the filter box above the configuration list, filter configurations by data ID, group, application, and label, and click 🔍 to display the configurations that meet the filter criteria.

----End

4.3.3.3 Viewing Configuration Details

You can view configuration details about a Nacos engine on the CSE console.

Step 1 **Log in to CSE**.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 In the left navigation pane, choose **Configuration Management** > **Configurations**.

Step 5 Click the target data ID. On the **Configuration Details** page displayed, view the configuration details. In the **Configuration Content** area, click **search** to query the configurations.

----End

4.3.3.4 Editing a Configuration

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 In the left navigation pane, choose **Configuration Management** > **Configurations**.

Step 5 Edit a configuration in either of the following methods:

- Click **Edit** in the **Operation** column of the target data ID.
- Click the target data ID. On the **Configuration Details** page displayed, click **Edit**.

Step 6 On the **Edit Configuration** page, modify the configuration content, format, description, application, and label. Click **Release**. The **Configuration Content Comparison** dialog box is displayed. You can view the differences between the historical and current versions.

Step 7 Click **Release**. The **Edit Configuration** page also provides dark launch. For details, see Configuring Dark Launch.

----End

4.3.3.5 Managing Historical Versions

CSE Nacos allows you to view details about historical versions and roll back historical versions.

Viewing Historical Versions

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 In the left navigation pane, choose **Configuration Management** > **Configurations**.

Step 5 Go to the **Historical Versions** page in either of the following methods. Click the data ID of a historical version in a time segment to view the historical version information of the configuration item.

- In the **Operation** column of the target data ID, choose **More** > **Historical Versions**.
- Click the target data ID. On the **Configuration Details** page displayed, click the **Historical Versions** tab.

NOTE

Historical versions can be retained for a maximum of 30 days.

----End

Rolling Back a Historical Version

CSE Nacos allows you to roll back a historical version to help you quickly restore incorrect configurations, reducing potential risks in configuration management of the microservice system.

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 In the left navigation pane, choose **Configuration Management** > **Configurations**.

Step 5 Go to the **Historical Versions** page in either of the following methods.

- In the **Operation** column of the target data ID, choose **More** > **Historical Versions**.
- Click the target data ID. On the **Configuration Details** page displayed, click the **Historical Versions** tab.

Step 6 Click **Roll Back** in the **Operation** column of the target historical version. The **Historical Version Details** page is displayed.

NOTE

Only the configuration whose **Operation** is **Update** can be rolled back.

Step 7 In the **Configuration Content** area, click **Roll Back to the Selected Version**. In the displayed dialog box, click **OK**.

----End

4.3.3.6 Importing/Exporting Configurations

CSE Nacos supports configuration import and export.

Importing Configurations

Step 1 Log in to CSE.

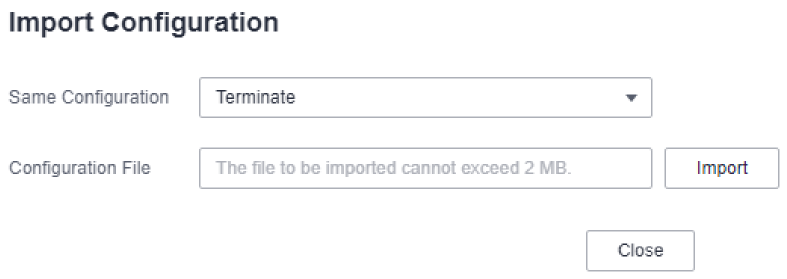
Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 In the left navigation pane, choose **Configuration Management** > **Configurations**.

Step 5 Click **Import Configuration** and set parameters by referring to the following table.

Figure 4-1 Importing configurations


Import Configuration

Same Configuration: Terminate

Configuration File: The file to be imported cannot exceed 2 MB.

Parameter	Description
Same Configuration	- **Terminate**: If a configuration is the same as that in the system, the import terminates. - **Skip**: During import, if a configuration is the same as that in the system, the configuration is skipped and other configurations are imported. - **Overwrite**: During import, if a configuration is the same as that in the system, the value of the configuration will be replaced.
Configuration File	Click **Import** and select the target file. **NOTE** The file size cannot exceed 2 MB. If the file is too large, divide it into smaller files and import them individually.

Step 6 Click **Close**.

NOTE

- If **Same Configuration** is **Terminate**, the **Terminate** dialog box will be displayed if a configuration is the same as that in the system during the import. Click **OK** to terminate the import.
- If **Same Configuration** is **Skip**, the configuration that is the same as that in the system will be skipped during the import, and other configurations are imported. Then, a dialog box is displayed showing the imported configurations. Click **OK**.

----End

Exporting Configurations

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

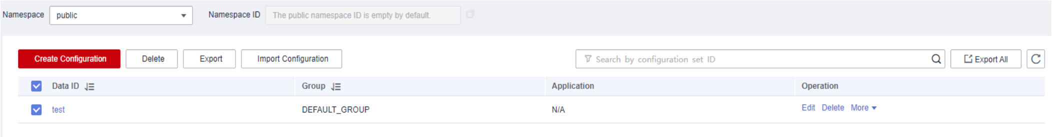
Step 4 In the left navigation pane, choose **Configuration Management** > **Configurations**.

Step 5 Select the target configuration and click **Export**.

NOTE

- Click **Export All** to export all configurations.
- You are advised to export the configurations separately to ensure that the size of an exported configuration file does not exceed 2 MB.

Figure 4-2 Exporting configurations



Namespace: public

Namespace ID: The public namespace ID is empty by default.

☑	Data ID	Group	Application	Operation
☑	test	DEFAULT_GROUP	N/A	Edit Delete More ▾

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

----End

4.3.3.7 Configuring Dark Launch

The CSE Nacos configuration center supports dark launch. That is, configurations can be partially verified before official release. After verification, configurations will be officially released to reduce the risk of configuration push.

Configuring Dark Launch

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 In the left navigation pane, choose **Configuration Management** > **Configurations**.

Step 5 Click **Edit** in the **Operation** column of the target configuration item.

Step 6 On the **Edit Configuration** page, click to enable dark launch.

Step 7 Select the IP address of the instance to be pushed in dark launch in the text box or manually enter the IP address of the instance for dark launch. Click **Enter**.

NOTE

Multiple instance IP addresses can be configured at the same time.

Step 8 Click **Release**. In the displayed **Configuration Content Comparison** dialog box, compare the configurations between the historical and current versions.

Step 9 Click **Release**.

----End

Viewing Dark Launch Version Configurations

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 In the left navigation pane, choose **Configuration Management** > **Configurations**.

Step 5 Click **Edit** in the **Operation** column of the target configuration item that is being dark launched.

Step 6 On the **Dark Launch Version** tab of the **Edit Configuration** page, you can view the dark launch version configuration, and roll back and release dark launch. For details, see **More Operations**.

----End

More Operations

- Roll back dark launch: On the **Dark Launch Version** tab of the **Edit Configuration** page, click **Roll Back** to cancel dark launch and roll back to the historical version.
- Release dark launch: On the **Dark Launch Version** tab of the **Edit Configuration** page, click **Release**. In the **Configuration Content Comparison** dialog box, confirm the configuration and click **Release**. The dark launch version becomes an official version.

4.3.3.8 Deleting a Configuration

Step 1 **Log in to CSE**.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

Step 4 In the left navigation pane, choose **Configuration Management** > **Configurations**.

Step 5 Delete a configuration in either of the following methods:

- Click **Delete** in the **Operation** column of the target data ID.
- Select the target data ID and click **Delete** above.

Step 6 Click **OK**.

----End

4.3.3.9 Querying Listening

CSE Nacos provides listening query. That is, after modifying a configuration, you need to check whether the modified configuration information has been pushed to the host that listens to the configuration. This helps you better check whether the configuration change has been pushed to the client.

Step 1 **Log in to CSE**.

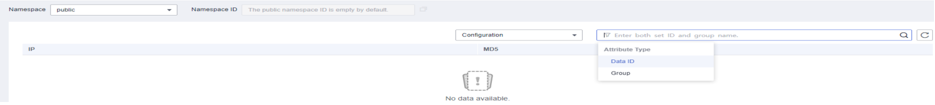
Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos instance.

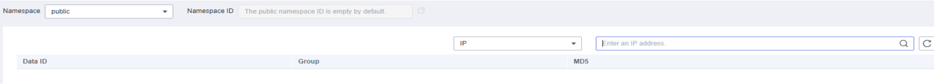
Step 4 In the left navigation pane, choose **Configuration Management** > **Listening Queries**.

Step 5 Select a namespace from the **Namespace** drop-down list, select search criteria, and click 🔍 to query listening information.

- If you select **Configuration** from the drop-down list, enter the data ID and group name in the text box to query the hosts to which the configuration is pushed and the push status.



- If you select **IP** from the drop-down list, enter the IP address of the listened host is configured in the text box to query all listened configurations of the host.



----End

4.3.4 Permission Control

4.3.4.1 Permission Control Overview

A Nacos engine may be used by many users. Exclusive Nacos engines with security authentication enabled provide permissions management using role-based access control (RBAC) on the microservice console, so that users have different engine access and operation permissions based on their responsibilities and permissions.

The Nacos engine with security authentication enabled supports microservice access.

NOTE

- Only engine 2.1.0.1 and later support this function. For engine earlier than 2.1.0.1, upgrade it to the latest version. For details, see **Upgrading a Nacos Engine**.
- If the Nacos engine version is upgraded from 2.1.0 to 2.1.0.1 or later, you need to enable security authentication to initialize the key information before using the permission control function.
- Eureka-compatible instances do not support security authentication.

4.3.4.2 Enabling and Disabling Security Authentication

Enabling Security Authentication

By default, security authentication is disabled for Nacos engines. You can enable security authentication on the console.

NOTE

After security authentication is enabled, only accessible namespaces are displayed on the console. Clients without usernames and passwords cannot access Nacos instances. Exercise caution when performing this operation.

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos engine.

Step 4 Choose **Permission Control**.

Step 5 Click **Set Authentication** and enable **Authenticate Programming Interface**.

Step 6 Click **OK**. After the Nacos engine is updated and the engine status changes from **Configuring** to **Available**, security authentication is enabled successfully.

----End

Disabling Security Authentication

NOTE

After security authentication is disabled, permissions of each user cannot be controlled. Clients can access Nacos instances without passwords, and all namespaces are displayed on the console. Exercise caution when performing this operation.

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos engine.

Step 4 Choose **Permission Control**.

Step 5 Click **Set Authentication**. On the **Security Settings** page, disable **Authenticate Programming Interface**.

Step 6 In the displayed dialog box, click **OK**. When the status of the engine changes to **Available**, security authentication is disabled.

----End

4.3.4.3 Accounts

You can log in to the engine console and create an account or manage a specified account created on the engine based on service requirements.

Creating an Account

Create an account and associates a proper role with the account. Users who use the account have the access and operation permissions on the Nacos engine.

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos engine.

Step 4 Choose **Permission Control**.

Step 5 Choose **Accounts** > **Create Account** and configure account parameters by referring to the following table:

Parameter	Description
Account	Enter an account name. **NOTE** The account name cannot be changed once the account is created.
Password	Enter a password.
Confirm Password	Enter the password again.

Step 6 Click **OK**.

----End

Resetting a Password

For security purposes, you can reset your password on the console.

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos engine.

Step 4 Choose **Permission Control**.

Step 5 On the **Accounts** tab page, click **Reset Password** in the **Operation** column of the target account.

Step 6 Enter and confirm a new password, select **I Understand**, and click **Save**.

----End

Deleting an Account

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos engine.

Step 4 Choose **Permission Control**.

Step 5 On the **Accounts** tab page, click **Delete** in the **Operation** column of the target account. In the displayed dialog box, enter **DELETE** and click **OK**.

----End

4.3.4.4 Roles

You can log in to the engine console and create, edit, delete, and view roles of a Nacos engine based on service requirements. Permission control by namespace or finer granularity is supported.

NOTE

If the Nacos engine is upgraded from an earlier version to 2.1.0.1, the system has the built-in role **ROLE_ADMIN** by default. The role cannot be deleted.

Creating a Role

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos engine.

Step 4 Choose **Permission Control**.

Step 5 On the **Roles** tab page, click **Create Role**.

Step 6 Enter a role name.

NOTE

The role name cannot be changed once the role is created.

Step 7 Set **Associated user**. Select the user created in **Creating an Account** from the drop-down list.

Step 8 Add permission configurations.

Click ⊕ **Add Permission Configuration** and select a namespace and action (**Read only**, **Write only**, or **Read/write**). You can add multiple permission configurations at a time or click **Delete** in the **Operation** column of a permission configuration to delete it.

NOTE

The role also has the permissions configured here.

Step 9 Click **Create**.

----End

Editing a Role

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos engine with security authentication enabled.

Step 4 Choose **Permission Control**.

Step 5 On the **Roles** tab page, click **Edit** in the **Operation** column of the role to be edited.

Step 6 Modify **Namespace** and **Action** based on service requirements.

Step 7 Click **Edit**.

----End

Deleting a Role

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos engine.

Step 4 Choose **Permission Control**.

Step 5 On the **Roles** tab, click **Delete** in the **Operation** column of the role to be deleted. In the displayed dialog box, enter **DELETE** and click **OK**.

> NOTE
>
> Deleted roles cannot be restored. Exercise caution when performing this operation.

----End

4.3.4.5 Console Resource Management

Nacos engines support the association between namespaces and enterprise projects. The relationship is N:1, that is, N namespaces can be associated with one enterprise project.

By default, the namespace created in **Creating a Namespace** is not associated with any enterprise project. You can associate the namespace with an enterprise project by editing the enterprise project.

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos engine.

Step 4 Choose **Permission Control**.

Step 5 On the **Console Resource Management** tab, click ✎ in the **Enterprise Project** column of the target namespace. In the **Edit Enterprise Project** dialog box, select an enterprise project from the drop-down list and click **OK**.

> NOTE
>
> When editing an enterprise project, you can only change the enterprise project and cannot leave the enterprise project empty.

----End

4.3.5 Viewing Monitoring of a Nacos Engine

When using the Nacos engine, you can view common metrics related to the Nacos engine in the configuration center and registry center on the running monitoring page provided by the CSE console. This section describes how to view monitoring metrics of Nacos engines.

> NOTE
>
> To view the running Nacos monitoring data, ensure that you have the AOM FullAccess permission.

Step 1 Log in to CSE.

Step 2 In the left navigation pane, choose **Registry/Configuration Center**.

Step 3 Click the target Nacos engine.

Step 4 In the left navigation pane, choose **Monitoring**. You can view Nacos monitoring metrics.

- On the **Dashboard** tab page, you can view **Microservice Instances** and **Configurations**. In addition, **Microservice Instance Use** and **Configuration Use** are displayed in graphics.
  - Microservice Instance Use: Ratio of the number of connected microservice instances to the recommended max. number of microservice instances. Increase instances for a high ratio.
  - Configuration Use: Ratio of created configurations to the max. configurations allowed.
- On the **Configuration Center Monitoring** tab page, you can select a time from the drop-down list in the upper right corner to view the monitoring data of the configuration center in a specified period, including Configurations, Long Connections, Write Request Frequency, Read Request Frequency, Average Response Time for Write Request, Average Response Time for Read Request, and Configuration Push Time Required. The value can be Last 30 minutes, Last 1 hour, Last 6 hours, Last 1 day, or Last week. By default, the monitoring data of the last 30 minutes is displayed.
- On the **Registry Center Monitoring** tab page, you can select a time from the drop-down list in the upper right corner to view the monitoring data of the registry center in a specified period, including Microservices, Microservice Instances, Write Request Frequency, Read Request Frequency, Average Response Time for Write Request, Average Response Time for Read Request, and Service Push Time Required. The value can be Last 30 minutes, Last 1 hour, Last 6 hours, Last 1 day, or Last week. By default, the monitoring data of the last 30 minutes is displayed.

----End

5 Key Operations Recorded by CTS

5.1 CSE Operations That Can Be Recorded by CTS

With Cloud Trace Service (CTS), you can query, audit, and review operations performed on cloud resources. Traces include the operation requests sent using the management console or APIs as well as the results of these requests.

To collect, record, or query operation logs of Nacos and ServiceComb engines, **enable CTS** first. With CTS, you can view operation records of Nacos and ServiceComb engines in the last seven days. **Table 5-1** and **Table 5-2** list the supported operation logs.

Table 5-1 Nacos engine operations that can be recorded by CTS

Operation	Resource Type	Event Name
Creating an engine	engine	CreateEngineJob
Deleting an engine	engine	DeleteEngineJob
Creating a service	service	createService
Modifying a service	service	modifyService
Deleting a service	service	deleteService
Releasing a configuration	config	publishConfig
Deleting a Configuration	config	deleteConfig
Creating a namespace	namespace	createNamespace
Modifying a namespace	namespace	modifyNamespace
Deleting a namespace	namespace	deleteNamespace

Table 5-2 ServiceComb engine operations that can be recorded by CTS

Operation	Resource Type	Event Name
Creating an engine	engine	createEngine
Deleting an engine	engine	deleteEngine
Upgrading or modifying an engine	engine	upgradeOrModifyEngine
Creating an engine backup task	engine	createEngine_backup
Deleting an engine backup task	engine	deleteEngine_backup
Creating an engine restoration task	engine	createEngine_recovery
Creating an engine backup policy	engine	createEngine_backup_strategy
Deleting an engine backup policy	engine	deleteEngine_backup_strategy
Updating an engine backup policy	engine	updateEngine_backup_strategy
Updating a dark launch rule	engine	ModifyDarklaunch
Deleting a dark launch rule	engine	DeleteDarklaunch
Modifying a configuration item	engine	ModifyConfig
Creating a configuration item	engine	CreateConfig
Deleting a configuration item	engine	DeleteConfig
Updating a governance rule	engine	ModifyGovern_policy
Updating a microservice	engine	modifyMicroservice
Creating a microservice	engine	createMicroservice
Deleting a microservice	engine	deleteMicroservice
Creating a microservice tag	engine	createMicroserviceTag
Updating a microservice tag	engine	updateMicroserviceTag

Operation	Resource Type	Event Name
Deleting a microservice tag	engine	deleteMicroserviceTag
Creating a microservice rule	engine	createMicroserviceRule
Updating a microservice rule	engine	updateMicroserviceRule
Deleting a microservice rule	engine	deleteMicroserviceRule
Creating a microservice schema	engine	createMicroserviceSchema
Updating a microservice schema	engine	updateMicroserviceSchema
Deleting a microservice schema	engine	deleteMicroserviceSchema
Updating microservice dependencies	engine	updateMicroserviceDependency
Updating microservice attributes	engine	updateMicroserviceProperty
Updating a microservice	engine	updateMicroservice
Updating monitoring thresholds	engine	updateThreshold
Updating a custom rule	engine	updateItem_meta
Deleting a custom rule	engine	DeleteItem_meta
Clearing configuration items	engine	executeConfig_cleanup
Updating status of a microservice instance	engine	updateInstanceStatus
Updating attributes of a microservice instance	engine	updateInstanceProperty
Creating a microservice instance	engine	createInstance
Deleting a microservice instance	engine	deleteInstance

5.2 Querying Real-Time Traces

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in OBS buckets. CTS stores operation records generated in the last seven days.

This section describes how to query and export operation records of the last seven days on the CTS console.

- **Viewing Real-Time Traces in the Trace List of the New Edition**
- **Viewing Real-Time Traces in the Trace List of the Old Edition**

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for more than seven days, you must configure an OBS bucket to transfer records to it. Otherwise, you cannot query the operation records generated seven days ago.
- After performing operations on the cloud, you can query management traces on the CTS console 1 minute later and query data traces on the CTS console 5 minutes later.

Viewing Real-Time Traces in the Trace List of the New Edition

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 **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
   - **Trace Name**: Enter a trace name.
   - **Trace ID**: Enter a trace ID.
   - **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
   - **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
   - **Trace Source**: Select a cloud service name from the drop-down list.
   - **Resource Type**: Select a resource type from the drop-down list.

   - **Operator**: Select one or more operators from the drop-down list.
   - **Trace Status**: Select **normal**, **warning**, or **incident**.
     - **normal**: The operation succeeded.
     - **warning**: The operation failed.
     - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
   - **Enterprise Project ID**: Enter an enterprise project ID.
   - **Access Key**: Enter an access key ID, including temporary access credentials and permanent access keys.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.

5. On the **Trace List** page, you can also export and refresh the trace list, and customize the list display settings.
   - Enter any keyword in the search box and press Enter to filter desired traces.
   - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5000 records.
   - Click ↻ to view the latest information about traces.
   - Click ⚙ to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled (●), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

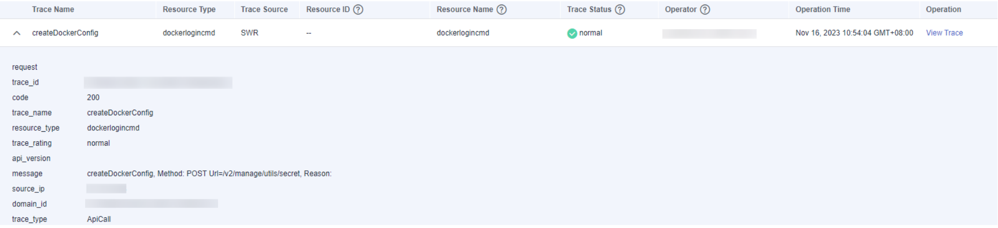
Viewing Real-Time Traces in the Trace List of the Old Edition

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 **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces. The following filters are available:
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
     - If you select **Resource ID** for **Search By**, specify a resource ID.
     - If you select **Trace name** for **Search By**, specify a trace name.

- If you select **Resource name** for **Search By**, specify a resource name.

- **Operator**: Select a user.
- **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
- Time range: You can query traces generated during any time range in the last seven days.
- Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.

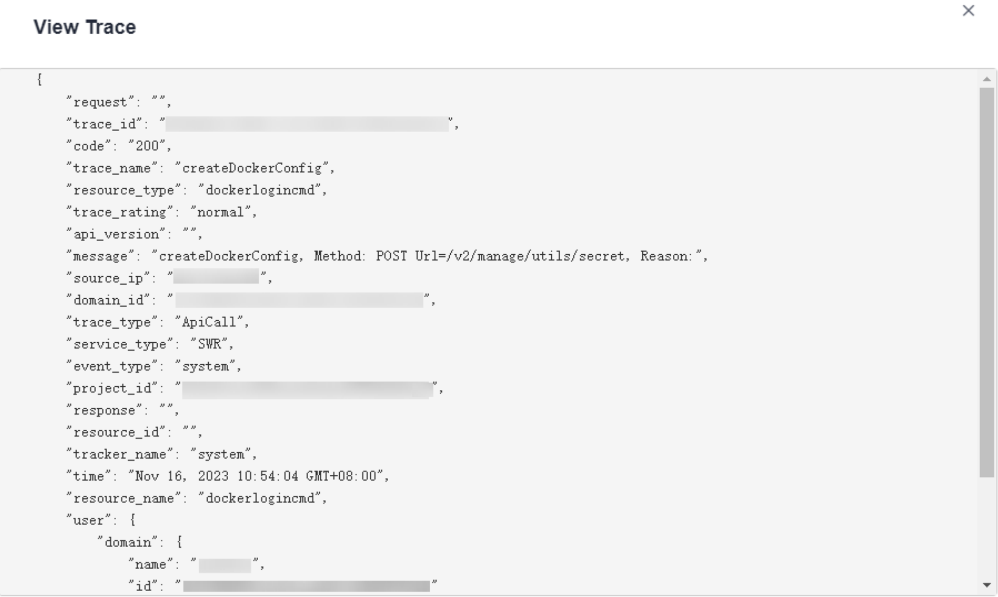
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
   - Click ↻ to view the latest information about traces.
8. Click ˅ on the left of a trace to expand its details.



	Trace Name	Resource Type	Trace Source	Resource ID	Resource Name	Trace Status	Operator	Operation Time	Operation
˄	createDockerConfig	dockerlogincmd	SWR	--	dockerlogincmd	✓ normal	[redacted]	Nov 16, 2023 10:54:04 GMT+08:00	View Trace

```
request
trace_id        [redacted]
code            200
trace_name      createDockerConfig
resource_type   dockerlogincmd
trace_rating    normal
api_version
message         createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:
source_ip       [redacted]
domain_id       [redacted]
trace_type      ApiCall
```

9. Click **View Trace** in the **Operation** column. The trace details are displayed.



View Trace

```
{
    ”request”: ””,
    ”trace_id”: ”[redacted]”,
    ”code”: ”200”,
    ”trace_name”: ”createDockerConfig”,
    ”resource_type”: ”dockerlogincmd”,
    ”trace_rating”: ”normal”,
    ”api_version”: ””,
    ”message”: ”createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:”,
    ”source_ip”: ”[redacted]”,
    ”domain_id”: ”[redacted]”,
    ”trace_type”: ”ApiCall”,
    ”service_type”: ”SWR”,
    ”event_type”: ”system”,
    ”project_id”: ”[redacted]”,
    ”response”: ””,
    ”resource_id”: ””,
    ”tracker_name”: ”system”,
    ”time”: ”Nov 16, 2023 10:54:04 GMT+08:00”,
    ”resource_name”: ”dockerlogincmd”,
    ”user”: {
        ”domain”: {
            ”name”: ”[redacted]”,
            ”id”: ”[redacted]”
```

10. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces** in the *CTS User Guide*.
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.