

ServiceStage

Best Practices

Issue 01
Date 2023-11-09



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. All rights reserved.

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

Trademarks and Permissions



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

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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Hosting and Managing a Weather Forecast Microservice Application on ServiceStage	1
1.1 Overview.....	1
1.2 Deploying a Weather Forecast Microservice Using Source Code.....	3
1.2.1 Preparations.....	3
1.2.2 Deploying a Microservice Using Source Code.....	7
1.3 Deploying a Weather Forecast Microservice Using a Software Package.....	16
1.3.1 Preparations.....	16
1.3.2 Deploying a Microservice Using a Software Package.....	21
1.4 Microservice Routine O&M.....	30
1.5 Dark Launch.....	31
1.6 Microservice Governance.....	34
1.7 FAQs.....	37
1.7.1 What Should I Do If a Weather Forecast Application with the Same Name Exists in the Current Environment?.....	38
2 Enabling Security Authentication for an Exclusive Microservice Engine	39
3 Connecting Microservice Engine Dashboard Data to AOM through ServiceStage	42
4 Migrating the Registered Microservice Engine Using ServiceStage Without Code Modification	45
5 Hosting a Spring Boot Application on ServiceStage	47
5.1 Preparations.....	47
5.2 Deploying and Accessing Spring Boot Applications.....	51
5.3 Upgrading Component Versions Using ELB Dark Launch.....	55
6 Using GitLab to Interconnect with Jenkins to Automatically Build and Upgrade Components Deployed on ServiceStage	57
6.1 Overview.....	57
6.2 Preparations.....	57
6.2.1 Preparing the Jenkins Environment.....	57
6.2.2 Uploading Code to GitLab.....	59
6.2.3 Installing and Initializing obsutil.....	59
6.2.4 Installing and Initializing KooCLI.....	60

6.2.5 Installing the Jenkins Plug-in and Configuring Jenkins.....	62
6.3 Procedure.....	64
6.3.1 Interconnection Tests.....	64
6.3.2 Configuring a Pipeline Build Task.....	65
6.3.3 upgrade.sh Description	67
6.4 Build Verification.....	72
6.4.1 Manual Build.....	72
6.4.2 Jenkins Build Triggered by GitLab.....	73

1 Hosting and Managing a Weather Forecast Microservice Application on ServiceStage

1.1 Overview

A weather forecast microservice application provides weather forecasts as well as displays ultraviolet (UV) and humidity indexes. This section uses a weather forecast application to demonstrate the application scenarios of the microservice architecture and best practices of managing the runtime environment, building applications, and governing microservices on ServiceStage.

A weather forecast microservice application consists of a frontend component and backend components. The frontend component **weathermapweb** is developed using Node.js to discover backend components. The backend components are developed using the Java chassis and Spring Cloud microservice development frameworks and include microservices weather, forecast, fusionweather, weather-beta, and edge-service.

Where,

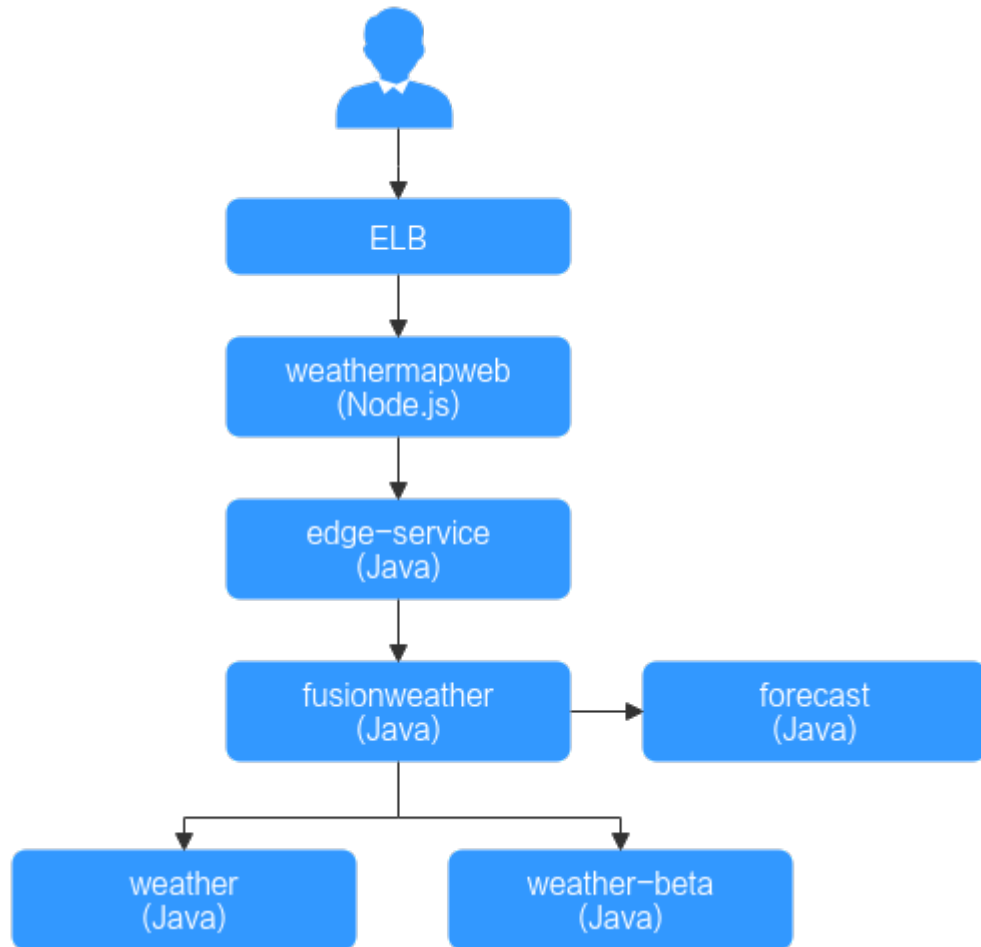
- weathermapweb is an interface microservice developed by Node.js.
- weather is a microservice that provides the current weather of a specified city.
- forecast is a microservice that provides weather forecast for a specified city in the next few days.
- fusionweather is an aggregation microservice that provides comprehensive weather forecast functions by accessing the weather and forecast microservices.
- weather-beta is a new version of the weather microservice. It allows you to query the UV index of a specified city.
- edge-service is the unified portal for all other microservices.

Table 1-1 lists the backend components.

Table 1-1 Components of the weather forecast microservice application

Microservice development framework	Component Name
Java Chassis	weather
	forecast
	fusionweather
	weather-beta
	edge-service
	weathermapweb
Spring Cloud	weather
	forecast
	fusionweather
	weather-beta
	edge-service
	weathermapweb

The following figure shows the logical networking and calling relationship of the weather forecast application:



ServiceStage supports deployment and access of microservice applications developed based on Java chassis and Spring Cloud using source code and software packages.

This document describes how to host and manage a microservice application on ServiceStage by using the weather forecast microservice application developed based on Java chassis and two microservice application deployment methods ([Deploying a Weather Forecast Microservice Using Source Code](#) and [Deploying a Weather Forecast Microservice Using a Software Package](#)).

1.2 Deploying a Weather Forecast Microservice Using Source Code

1.2.1 Preparations

Preparing Resources

To facilitate subsequent operations, ensure that:

1. You have created a Virtual Private Cloud (VPC). For details, see [Creating a VPC](#).

2. You have created an exclusive microservice engine with security authentication disabled. For details, see [Creating a Microservice Engine](#).
 - The VPC to which the microservice engine belongs is the one created in [1](#). If the VPCs are inconsistent, correctly configure the VPC connectivity.
 - If you have [enabled the enterprise project function](#), the microservice engine and its VPC must be in the same enterprise project.
3. You have created a Cloud Container Engine (CCE) cluster. In a trial scenario, set **Management Scale** to **50 nodes** and **HA** to **No**.

The cluster contains at least one ECS node with 8 vCPUs and 16 GB memory or two ECS nodes with 4 vCPUs and 8 GB memory, and is bound to an EIP. For details, see [Buying a Cluster](#).

 - The VPC to which the CCE cluster belongs is the one created in [1](#).
 - If you have [enabled the enterprise project function](#), the CCE cluster and its VPC must be in the same enterprise project.
 - The CCE cluster cannot be bound to other environments.
 - If a CCE cluster 1.23 or later is created, **Container Engine** of the ECS node in the cluster supports only Docker.
4. In this example, the GitHub source code repository is bound to ServiceStage to implement source code building, archiving, and application creation. Ensure that you have registered an account on [GitHub](#).

Forking the Weather Forecast Source Code

Use your account to log in to GitHub and fork the weather forecast source code. Source code address: <https://github.com/servicestage-demo/weathermap.git>

Setting GitHub Repository Authorization

You can set GitHub repository authorization so that build projects and application components can use the authorization information to access the GitHub source code repository.

Step 1 Log in to ServiceStage.

Step 2 Choose **Continuous Delivery > Repository Authorization > Create Authorization** and configure authorization information by referring to the following table. Parameters marked with an asterisk (*) are mandatory.

Parameter	Description
*Name	Use the default authorization name. This name cannot be changed after being created.
*Repository Authorization	<ol style="list-style-type: none">1. Select GitHub.2. Select an authorization method.<ul style="list-style-type: none">– OAuth: Click Use OAuth Authorization and complete the authorization creation as prompted.– Personal token: Enter the obtained private token and click Create.

Step 3 Click **Create**.

----End

Creating an Organization

Step 1 Choose **Deployment Source Management > Organization Management**.

Step 2 Click **Create Organization**. On the displayed page, specify **Organization Name**. For example, **org-test**.

Step 3 Click **OK**.

Figure 1-1 Creating an organization

Create Organization

- Each organization name must be globally unique.
- The current account can create a maximum of 5 organizations.
- For centralized management of images, limit each organization to one company, department, or individual.

Example:

Company or department: cloud-hangzhou or cloud-develop

Person: john

* Organization Name

org-test

OK

Cancel

----End

Creating an Environment

Step 1 Choose **Environment Management > Create Environment** and set the environment information by referring to the following table.

Parameter	Description
Environment	Enter an environment name, for example, env-test .
Enterprise Project	Specify Enterprise Project . Enterprise projects let you manage cloud resources and users by project. It is available after you enable the enterprise project function . The environment and its VPC must be in the same enterprise project.
Description	Retain the default value.

Parameter	Description
VPC	Select the VPC prepared in Preparing Resources . NOTE The VPC cannot be modified after the environment is created.
Environment Type	Select Kubernetes .

Figure 1-2 Configuring an environment

The screenshot displays the configuration form for a new environment. It includes the following elements:

- Environment:** A text input field containing 'env-test'.
- Enterprise Project:** A dropdown menu showing 'default' and a 'Create Enterprise Project' button.
- Description:** A field with a placeholder '--' and an edit icon.
- VPC:** A dropdown menu showing 'vpc-test' and a 'Create a VPC' button.
- Environment Type:** Two buttons: 'VM' and 'Kubernetes' (which is highlighted in blue).

Step 2 Click **Create Now**.

Step 3 In the **Resource Settings** area, choose **Cloud Container Engine** from **Compute** and click **Bind now**.

Step 4 In the dialog box that is displayed, select the CCE cluster created in [Preparing Resources](#) and click **OK**.

Step 5 In the **Resource Settings** area, choose **Cloud Service Engine** from **Middleware** and click **Manage Resource**.

Step 6 In the dialog box that is displayed, select the microservice engine created in [Preparing Resources](#) and click **OK**.

----End

Creating an Application

Step 1 Click in the upper left corner to return to the **Environment Management** page.

Step 2 Choose **Application Management** > **Create Application** and set basic application information.

1. **Name:** Enter **weathermap**.

NOTE

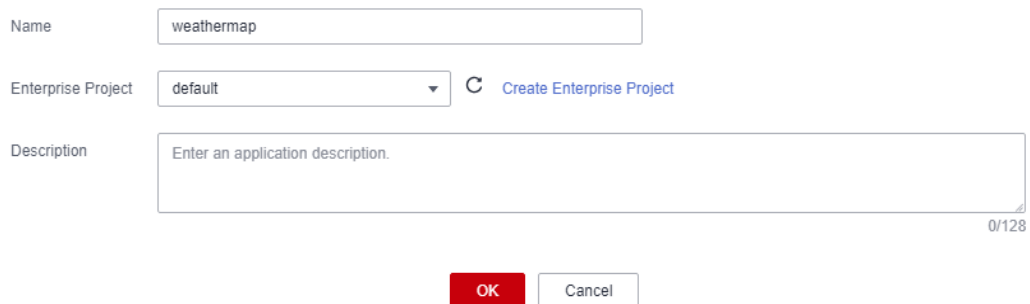
If an application with the same name already exists in the application list, rectify the fault by referring to [What Should I Do If a Weather Forecast Application with the Same Name Exists in the Current Environment?](#).

2. **Enterprise Project:** Enterprise projects let you manage cloud resources and users by project.

It is available after you [enable the enterprise project function](#). The application and the [created environment](#) must be in the same enterprise project.

Step 3 Click **OK**.

Figure 1-3 Creating an application

Create Application

Name: weathermap

Enterprise Project: default [Create Enterprise Project](#)

Description: Enter an application description. 0/128

OK Cancel

----End

1.2.2 Deploying a Microservice Using Source Code

Scenarios

ServiceStage allows you to quickly deploy microservices in containers (such as CCE) or VMs (such as ECS), and supports source code deployment, JAR/WAR package deployment, and Docker image package deployment. In addition, ServiceStage allows you to deploy, upgrade, roll back, start, stop, and delete applications developed in different programming languages, such as Java, PHP, Node.js, and Python.

In this practice, backend components developed in Java and frontend components developed in Node.js are used.

User Story

In this practice, you can deploy an application in containers and register microservice instances with the microservice engine. The following components need to be created for the weathermap application:

1. Frontend component: weathermapweb, which is developed in Node.js.
2. Backend components: weather, fusionweather, forecast, and edge-service, which are developed based on Java.

The procedures for deploying a microservice are as follows:

1. [Creating and Deploying a Backend Application Component](#)
2. [Setting the Access Mode of the edge-service Component](#)
3. [Creating and Deploying a Frontend Component](#)
4. [Confirming the Deployment Result](#)
5. [Setting the Access Mode](#)
6. [Accessing an Application](#)

Creating and Deploying a Backend Application Component

You need to create and deploy four application components (weather, forecast, fusionweather, and edge-service), which correspond to the four software packages generated by the backend build jobs.

Step 1 Log in to ServiceStage.

Step 2 Choose **Application Management**. The application list is displayed.

Step 3 Click **Create Component** in the **Operation** column of the application created in [Creating an Application](#) (for example, **weathermap**).

Step 4 In the **Basic Information** area, set the following mandatory parameters. Retain the default values for other parameters.

Parameter	Description
Component Name	Enter the name of the corresponding backend component (for example, weather).
Component Version	Click Generate . By default, the version number is generated based on the time when you click Generate . The format is yyyy.mmdd.hhmms , in which s is the ones digit of second in the timestamp. For example, if the timestamp is 2022.0803.104321, the version number is 2022.0803.10431.
Environment	Select the environment created in Creating an Environment , for example, env-test .
Application	Select the application created in Creating an Application , for example, weathermap .

Step 5 In the **Component Package** area, set the following mandatory parameters. Retain the default values for other parameters.

Parameter	Description
Stack	Select Java .

Parameter	Description
Source Code/ Software Package	<ol style="list-style-type: none"> 1. Select Source code repository and GitHub. 2. Authorization: Select the authorization information created in Setting GitHub Repository Authorization. 3. Username/Organization: Select the username used to log in to GitHub in Forking the Weather Forecast Source Code. 4. Repository: Select the name of the weather forecast source code repository that has been forked to your GitHub account. For example, weathermap. 5. Branch: Select master.

Step 6 In the **Build Job** area, set mandatory build parameters.

1. **Command**: Retain the default value.
2. **Dockerfile Address**: Set this parameter by referring to the following table.

Component Name	Dockerfile Address
weather	./weather/
forecast	./forecast/
fusionweather	./fusionweather/
edge-service	./edge-service/

3. **Organization**: Select the organization created in [Creating an Organization](#).
4. **Environment**: Select **Use current environment**.
5. Retain the default values for other parameters.

Figure 1-4 Configuring build parameters

The screenshot shows the 'Build Job' configuration page. It includes the following fields and options:

- Command**: Two tabs, 'Default command or script' (selected) and 'Custom command'.
- Dockerfile Address**: A text input field containing './weather/'.
- Organization**: A dropdown menu showing 'org-test'.
- Build**: Two buttons, 'Use independent environment' and 'Use current environment' (selected).
- Environment**: A dropdown menu showing 'env-cca'.
- Node Label**: Two dropdown menus, both showing '--Select key--' and '--Select value--'.

Below the Environment field, there is a note: "Must be a Kubernetes environment with internet access". Below the Node Label fields, there is a note: "Select a node that has an EIP bound and can access the public network. If such a node does not exist, refer to [Enabling Internet Connectivity for an ECS Without an EIP](#) and create one. If the node does not have a label, [create a label](#)."

Step 7 Click **Next**.

Step 8 In the **Resources** area, set **Instances** for each component and retain the default values for other parameters.

Component Name	Instances
weather	2
forecast	1
fusionweather	1
edge-service	1

Step 9 In the **Access Mode** area, retain the default settings.

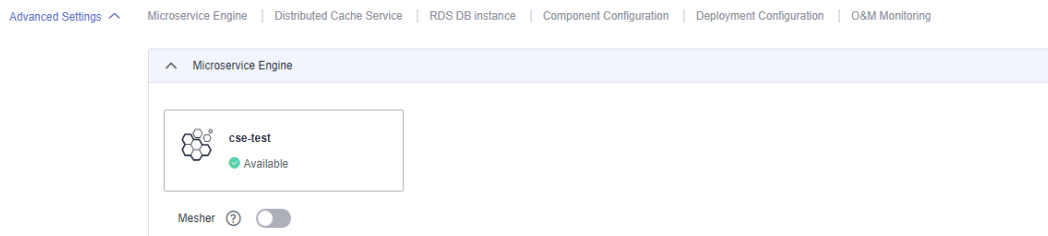
Step 10 In the **Local Time** area, retain the default settings.

Step 11 Bind a microservice engine.

 **NOTE**

- After a component is deployed, the microservice is registered with the microservice engine.
 - All components must be registered with the same microservice engine.
1. In the **Advanced Settings** area, expand **Microservice Engine**.
 2. Click **Bind Microservice Engine**.
 3. Select the managed microservice engine in the current environment.
 4. Click **OK**.


Figure 1-5 Binding a microservice engine



Step 12 Click **Create and Deploy**.

----End

Setting the Access Mode of the edge-service Component

Step 1 Click  in the upper left corner to return to the **Application Management** page.

Step 2 Click the application created in **Creating an Application** (for example, **weathermap**). The **Overview** page is displayed.

Step 3 In the **Component List** area, locate the row that contains **edge-service** and click **View Access Mode** in the **External Access Address** column.

Step 4 Click **Add Service** in the **TCP/UDP Route Configuration** area and set parameters by referring to the following table.

Parameter	Description
Service Name	Retain the default value.
Access Mode	Select Public network access .
Access Type	Select Elastic IP address .
Service Affinity	Retain the default value.
Protocol	Select TCP .
Container Port	Enter 3010 .
Access Port	Select Automatically generated .

Figure 1-6 Setting the access mode of the edge-service component

Add Service

★ Service name

Access Mode Intra-cluster access Intra-VPC access Public network access
Allows access from the Internet over TCP/UDP, including EIP.

★ Access Type

Container Port Cluster level Node level
1. All nodes in the cluster can use their IP addresses+port numbers to access the workload targeted by the service.
 2. Routing hops will be used. As a result, routing performance will be compromised and clients' source IP addresses will be masked.


★ Port Mapping

Protocol	Container Port	Access Port
<input type="text" value="TCP"/>	<input type="text" value="3010"/>	<input type="text" value="Automatically ..."/>

Step 5 Click **OK**.

----End

Creating and Deploying a Frontend Component

- Step 1** Click  in the upper left corner to return to the **Application Management** page.
- Step 2** Click **Create Component** in the **Operation** column of the application created in **Creating an Application** (for example, **weathermap**).
- Step 3** In the **Basic Information** area, set the following mandatory parameters. Retain the default values for other parameters.

Parameter	Description
Component Name	Enter the frontend component name weathermapweb .
Component Version	Click Generate . By default, the version number is generated based on the time when you click Generate . The format is yyyy.mmdd.hhmms , in which s is the ones digit of second in the timestamp. For example, if the timestamp is 2022.0803.104321, the version number is 2022.0803.10431.
Environment	Select the environment created in Creating an Environment , for example, env-test .
Application	Select the application created in Creating an Application , for example, weathermap .

Step 4 In the **Component Package** area, set the following mandatory parameters. Retain the default values for other parameters.

Parameter	Description
Stack	Select Node.js .
Source Code/ Software Package	<ol style="list-style-type: none"> 1. Select Source code repository and GitHub. 2. Authorization: Select the authorization information created in Setting GitHub Repository Authorization. 3. Username/Organization: Select the username used to log in to GitHub in Forking the Weather Forecast Source Code. 4. Repository: Select the name of the weather forecast source code repository that has been forked to your GitHub account. For example, weathermap. 5. Branch: Select master.

Step 5 In the **Build Job** area, set mandatory build parameters.

1. **Command**: Retain the default value.
2. **Dockerfile Address**: Set this parameter by referring to the following table.

Component Name	Dockerfile Address
weathermapweb	./weathermapweb/

3. **Organization**: Select the organization created in [Creating an Organization](#).
4. **Environment**: Select **Use current environment**.
5. Retain the default values for other parameters.

Step 6 Click **Next**.

Step 7 In the **Resources** area, retain the default settings.

Step 8 In the **Access Mode** area, retain the default settings.

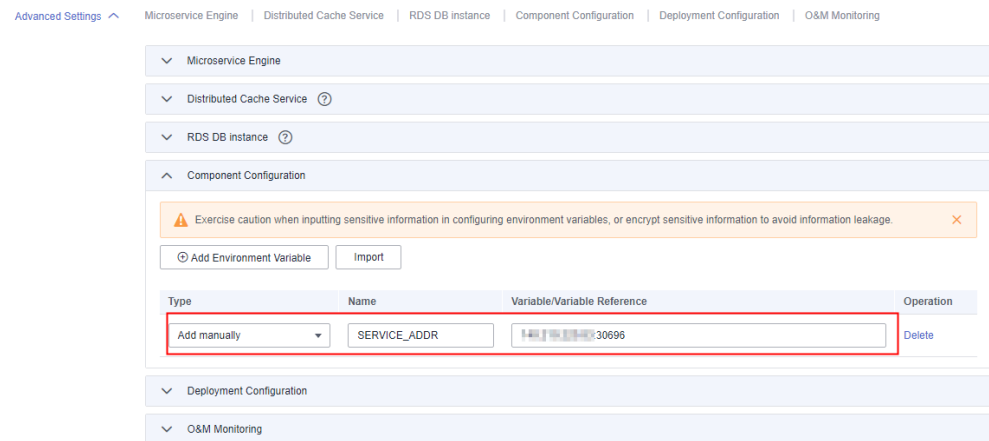
Step 9 In the **Local Time** area, retain the default settings.

Step 10 Add environment variables.

1. In the **Advanced Settings** area, expand **Component Configuration**.
2. Click **Add Environment Variable** to configure environment variables.

Type	Name	Variable/Variable Reference
Add manually	SERVICE_ADDR	Access address generated in Setting the Access Mode of the edge-service Component .

Figure 1-7 Adding environment variables



Step 11 Click **Create and Deploy**.

----End

Confirming the Deployment Result

Step 1 Click in the upper left corner to return to the **Application Management** page.

Step 2 Choose **Cloud Service Engine > Microservice Catalog**.

Step 3 Select the microservice engine where the microservice application is deployed from the **Microservice Engine** drop-down list.

Step 4 On the **Microservice List** tab, select **weathermap** from the **All applications** drop-down list.

If the number of instances of each microservice is the same as listed in the following table, the deployment is successful.

Component Name	Instances
weather	2

Component Name	Instances
forecast	1
fusionweather	1
edge-service	1

----End

Setting the Access Mode

- Step 1** Choose **Application Management**.
- Step 2** Click the application created in [Creating an Application](#) (for example, **weathermap**). The **Overview** page is displayed.
- Step 3** In the **Component List** area, locate the row that contains **weathermapweb** and click **View Access Mode** in the **External Access Address** column.
- Step 4** Click **Add Service** in the **TCP/UDP Route Configuration** area and set parameters by referring to the following table.

Parameter	Description
Service Name	Retain the default value.
Access Mode	Select Public network access .
Access Type	Select Elastic IP address .
Service Affinity	Retain the default value.
Protocol	Select TCP .
Container Port	Enter 3000 .
Access Port	Select Automatically generated .

Figure 1-8 Setting the access mode

✕

Add Service

* Service name

Access Mode Intra-cluster access Intra-VPC access Public network access
Allows access from the Internet over TCP/UDP, including EIP.

* Access Type

Container Port Cluster level Node level
 1. All nodes in the cluster can use their IP addresses+port numbers to access the workload targeted by the service.
 2. Routing hops will be used. As a result, routing performance will be compromised and clients' source IP addresses will be masked.

* Port Mapping

Protocol	Container Port	Access Port
TCP	3000	Automatically ...

Step 5 Click **OK**.


Figure 1-9 Access address

TCP/UDP Route Configuration Supports Layer-4 TCP/UDP load balancing

Internal Domain Name Access Address	Access Address	Access Mode	Protocol	Container Port	Access Port	Operation
weathermapweb.default.svc.cluster.local:3000	<input type="text" value="弹性公网IP:32314"/>	Public network access → EIP	TCP	3000	32314	Edit Delete

----End

Accessing an Application

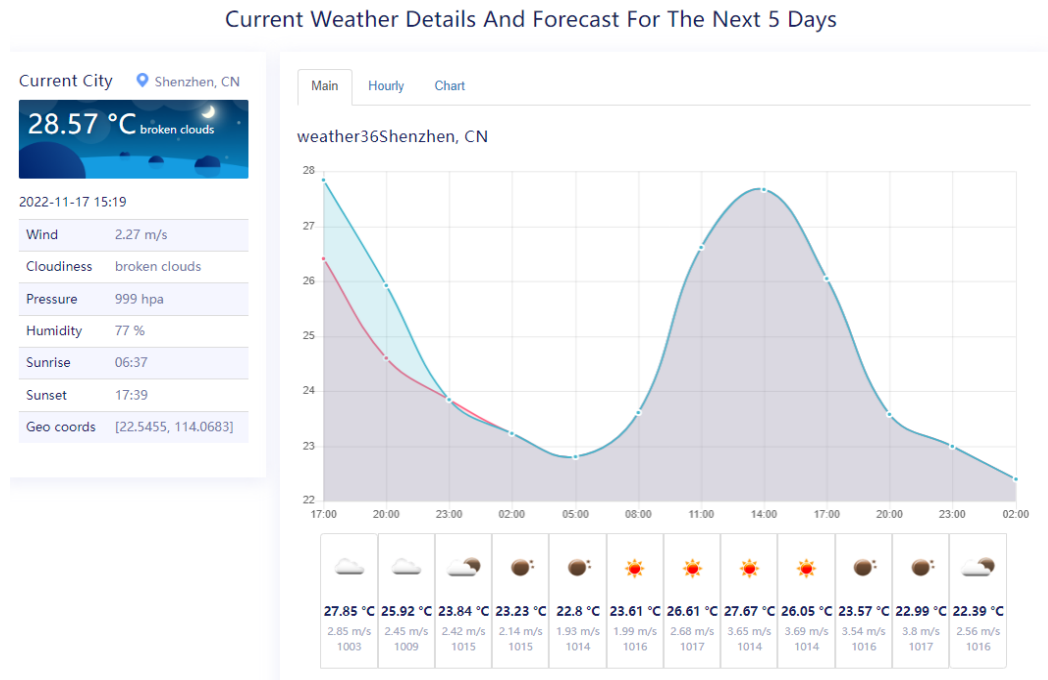
Step 1 Click  in the upper left corner to return to the **Application Management** page.

Step 2 Click the application created in [Creating an Application](#) (for example, **weathermap**). The **Overview** page is displayed.

Step 3 In the **Component List** area, locate the row that contains **weathermapweb** and click **View Access Mode** in the **External Access Address** column.

If the following page is displayed, the weather forecast microservice application is successfully deployed.

Figure 1-10 Application deployed successfully



NOTE

- The data is real-time data.
- When you access the application for the first time, it takes some time for the weather system to be ready. If the preceding page is not displayed, refresh the page.

----End

1.3 Deploying a Weather Forecast Microservice Using a Software Package

1.3.1 Preparations

Preparing Resources

To facilitate subsequent operations, ensure that:

1. You have created a VPC. For details, see [Creating a VPC](#).
2. You have created an exclusive microservice engine 2.4.0 or later with security authentication disabled. For details, see [Creating a Microservice Engine](#).
 - The VPC to which the microservice engine belongs is the one created in **1**. If the VPCs are inconsistent, correctly configure the VPC connectivity.
 - If you have [enabled the enterprise project function](#), the microservice engine and its VPC must be in the same enterprise project.
3. You have created a Cloud Container Engine (CCE) cluster. In a trial scenario, set **Management Scale** to **50 nodes** and **HA** to **No**.

The cluster contains at least one ECS node with 8 vCPUs and 16 GB memory or two ECS nodes with 4 vCPUs and 8 GB memory, and is bound to an EIP. For details, see [Buying a Cluster](#).

- The VPC to which the CCE cluster belongs is the one created in [1](#).
 - If you have [enabled the enterprise project function](#), the CCE cluster and its VPC must be in the same enterprise project.
 - The CCE cluster cannot be bound to other environments.
 - If a CCE cluster 1.23 or later is created, **Container Engine** of the ECS node in the cluster supports only Docker.
4. Create a bucket for storing software packages. For details, see [Creating a Bucket](#).

Downloading and Uploading Component Software Packages

- Step 1** Download the weather forecast component software package to the local PC by referring to [Table 1-2](#). (This practice uses the component developed based on Java chassis.)

Table 1-2 Software packages of the weather forecast components

Microservice Development Framework	Component Name	Component Software Package Name	Description of Downloading a Component Software Package
Java Chassis	weather	weather-1.0.0.jar	<ol style="list-style-type: none"> 1. Access software package repository of weather forecast components. 2. Click ServiceComb to access the software package repository of weather forecast components developed using the Java chassis microservice development framework.
	weather-beta	weather-beta-2.0.0.jar	
	forecast	forecast-1.0.0.jar	
	fusionweather	fusionweather-1.0.0.jar	
	edge-service	edge-service-1.0.0.jar	
	weathermapweb	weathermapweb.zip	

Microservice Development Framework	Component Name	Component Software Package Name	Description of Downloading a Component Software Package
Spring Cloud	weather	weather-1.0.0.jar	<ol style="list-style-type: none"> 1. Access software package repository of weather forecast components. 2. Click Spring Cloud to access the software package repository of weather forecast components developed using the Spring Cloud microservice development framework.
	weather-beta	weather-beta-2.0.0.jar	
	forecast	forecast-1.0.0.jar	
	fusionweather	fusionweather-1.0.0.jar	
	edge-service	edge-service-1.0.0.jar	
	weathermapweb	weathermapweb.zip	

Step 2 Upload the preceding software packages to the bucket prepared in [Preparing Resources](#).

Upload the software package. For details, see [Uploading an Object](#).

----End

Creating an Organization

Step 1 Log in to ServiceStage.

Step 2 Choose **Deployment Source Management > Organization Management**.

Step 3 Click **Create Organization**. On the displayed page, specify **Organization Name**. For example, **org-test**.

Step 4 Click **OK**.

Figure 1-11 Creating an organization

Create Organization

- Each organization name must be globally unique.
- The current account can create a maximum of 5 organizations.
- For centralized management of images, limit each organization to one company, department, or individual.

Example:

Company or department: cloud-hangzhou or cloud-develop

Person: john

★ Organization Name

----End

Creating an Environment

Step 1 Choose **Environment Management > Create Environment** and set the environment information by referring to the following table.

Parameter	Description
Environment	Enter an environment name, for example, env-test .
Enterprise Project	Set the enterprise project. The default value is used by default. It is available after the enterprise project function is enabled.
Description	Retain the default value.
VPC	Select the VPC prepared in Preparing Resources . NOTE <ul style="list-style-type: none"> • The VPC cannot be modified after the environment is created. • After a VPC is selected, resources in the VPC are loaded for selection. Resources that are not in the VPC cannot be selected.
Environment Type	Select Kubernetes .

Figure 1-12 Configuring an environment

The screenshot displays the configuration interface for creating an environment in ServiceStage. It includes the following elements:

- Environment:** A text input field containing "env-test".
- Enterprise Project:** A dropdown menu showing "default" and a "Create Enterprise Project" button.
- Description:** A field with a placeholder "--" and an edit icon.
- VPC:** A dropdown menu showing "vpc-test" and a "Create a VPC" button.
- Environment Type:** Two buttons, "VM" and "Kubernetes", with "Kubernetes" selected.

Step 2 Click **Create Now**.

Step 3 In the **Resource Settings** area, choose **Cloud Container Engine** from **Compute** and click **Bind now**.


Step 4 In the dialog box that is displayed, select the CCE cluster created in **Preparing Resources** and click **OK**.

Step 5 In the **Resource Settings** area, choose **Cloud Service Engine** from **Middleware** and click **Manage Resource**.

Step 6 In the dialog box that is displayed, select the microservice engine created in **Preparing Resources** and click **OK**.

----End

Creating an Application

Step 1 Click  in the upper left corner to return to the **Environment Management** page.

Step 2 Choose **Application Management** > **Create Application** and set basic application information.

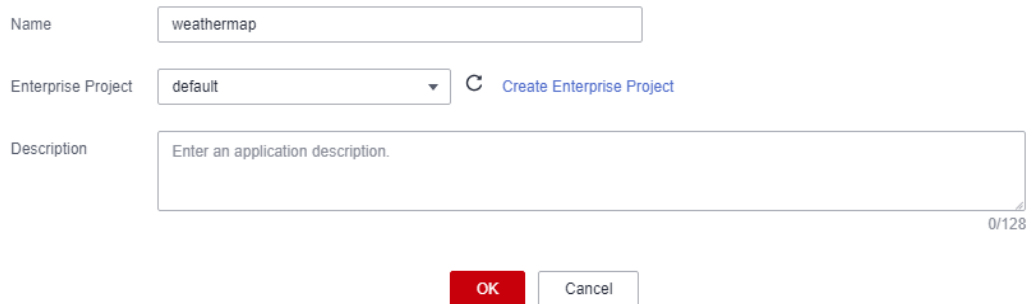
1. **Name:** Enter **weathermap**.

 **NOTE**

If an application with the same name already exists in the application list, rectify the fault by referring to [What Should I Do If a Weather Forecast Application with the Same Name Exists in the Current Environment?](#)

2. **Enterprise Project:** Select **default**. (This parameter is displayed only when the **enterprise project function** is enabled.)

Step 3 Click **OK**.

Figure 1-13 Creating an application**Create Application**

Name

Enterprise Project [Create Enterprise Project](#)

Description 0/128

----End

1.3.2 Deploying a Microservice Using a Software Package

Scenarios

ServiceStage allows you to quickly deploy microservices in containers (such as CCE) or VMs (such as ECS), and supports source code deployment, JAR/WAR package deployment, and Docker image package deployment. In addition, ServiceStage allows you to deploy, upgrade, roll back, start, stop, and delete applications developed in different programming languages, such as Java, PHP, Node.js, and Python.

In this practice, backend components developed in Java and frontend components developed in Node.js are used.

User Story

In this practice, you can deploy an application in containers and register microservice instances with the microservice engine. The following components need to be created and deployed for the weathermap application:

1. Frontend component: weathermapweb, which is developed in Node.js.
2. Backend components: weather, fusionweather, forecast, and edge-service, which are developed based on Java.

The procedures for deploying a microservice are as follows:

1. [Creating and Deploying a Backend Application Component](#)
2. [Setting the Access Mode of the edge-service Component](#)
3. [Creating and Deploying a Frontend Component](#)
4. [Confirming the Deployment Result](#)
5. [Setting the Access Mode](#)
6. [Accessing an Application](#)

Creating and Deploying a Backend Application Component

You need to create and deploy four application components (weather, forecast, fusionweather, and edge-service), which correspond to the four software packages generated by the backend build jobs.

Step 1 Log in to ServiceStage.

Step 2 Choose **Application Management**. The application list is displayed.

Step 3 Click **Create Component** in the **Operation** column of the application created in [Creating an Application](#) (for example, **weathermap**).

Step 4 In the **Basic Information** area, set the following mandatory parameters. Retain the default values for other parameters.

Parameter	Description
Component Name	Enter the name of the corresponding backend component (for example, weather).
Component Version	Click Generate . By default, the version number is generated based on the time when you click Generate . The format is yyyy.mmdd.hhmms , in which s is the ones digit of second in the timestamp. For example, if the timestamp is 2022.0803.104321, the version number is 2022.0803.10431.
Environment	Select the environment created in Creating an Environment , for example, env-test .
Application	Select the application created in Creating an Application , for example, weathermap .

Step 5 In the **Component Package** area, set the following mandatory parameters. Retain the default values for other parameters.

Parameter	Description
Stack	Select Java .
Upload Method	Click Select Software Package and select the uploaded software package of the corresponding component by referring to Table 1-2 .

Step 6 In the **Build Job** area, set the following mandatory parameters. Retain the default values for other parameters.

Parameter	Description
Organization	An organization is used to manage images generated during component building. Select the organization created in Creating an Organization .

Parameter	Description
Environment	Select Use current environment to use the CCE cluster in the deployment environment to which the component belongs to build an image. In the current environment, masters and nodes in the CCE cluster must have the same CPU architecture. Otherwise, the component build fails.

Step 7 Click **Next**.

Step 8 In the **Resources** area, set **Instances** for each component and retain the default values for other parameters.

Component Name	Instances
weather	2
forecast	1
fusionweather	1
edge-service	1

Step 9 In the **Access Mode** area, retain the default settings.

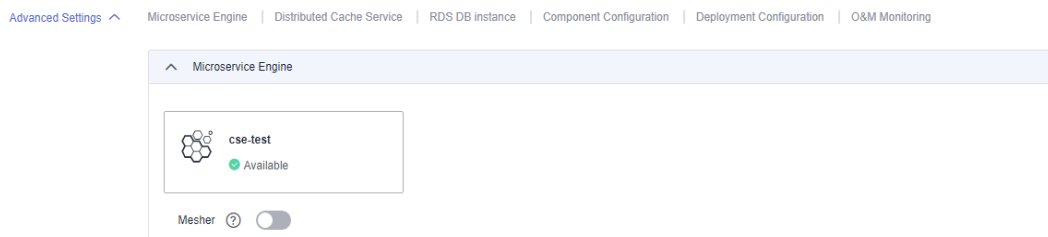
Step 10 In the **Local Time** area, retain the default settings.

Step 11 Bind a microservice engine.

 **NOTE**

- After a component is deployed, the microservice is registered with the microservice engine.
 - All components must be registered with the same microservice engine.
1. In the **Advanced Settings** area, expand **Microservice Engine**.
 2. Click **Bind Microservice Engine**.
 3. Select the managed microservice engine in the current environment.
 4. Click **OK**.

Figure 1-14 Binding a microservice engine



Step 12 (Optional) In the **Advanced Settings** area, choose **Advanced Settings > Component Configuration**, and click **Add Environment Variable** to add

environment variables for components **weather**, **forecast**, and **fusionweather** by referring to the following table.

Type	Name	Variable/Variable Reference
Add manually	MOCK_ENABLED	<p>Set the parameter value to false.</p> <ul style="list-style-type: none"> • true: If no EIP is bound to the ECS node in the CCE cluster created in Preparing Resources or the node cannot access the public network, set this parameter to true. The weather data used by the application is simulated data. • false: If an EIP has been bound to the ECS node in the CCE cluster created in Preparing Resources and the node can access the public network, set this parameter to false or do not set this parameter. The weather data used by the application is real-time data.

Step 13 Click **Create and Deploy**.

----End

Setting the Access Mode of the edge-service Component

Step 1 Click  in the upper left corner to return to the **Application Management** page.

Step 2 Click the application created in [Creating an Application](#) (for example, **weathermap**). The **Overview** page is displayed.

Step 3 In the **Component List** area, locate the row that contains **edge-service** and click **View Access Mode** in the **External Access Address** column.

Step 4 Click **Add Service** in the **TCP/UDP Route Configuration** area and set parameters by referring to the following table.

Parameter	Description
Service Name	Retain the default value.
Access Mode	Select Public network access .
Access Type	Select Elastic IP address .
Service Affinity	Retain the default value.

Parameter	Description
Protocol	Select TCP .
Container Port	Enter 3010 .
Access Port	Select Automatically generated .

Figure 1-15 Setting the access mode of the edge-service component

Add Service

★ Service name

Access Mode Intra-cluster access Intra-VPC access Public network access
Allows access from the Internet over TCP/UDP, including EIP.

★ Access Type

Container Port Cluster level Node level
1. All nodes in the cluster can use their IP addresses+port numbers to access the workload targeted by the service.
 2. Routing hops will be used. As a result, routing performance will be compromised and clients' source IP addresses will be masked.


★ Port Mapping

Protocol	Container Port	Access Port
<input type="text" value="TCP"/>	<input type="text" value="3010"/>	<input type="text" value="Automatically ..."/>

Step 5 Click **OK**.

----End

Creating and Deploying a Frontend Component

Step 1 Click  in the upper left corner to return to the **Application Management** page.

Step 2 Click **Create Component** in the **Operation** column of the application created in [Creating an Application](#) (for example, **weathermap**).

Step 3 In the **Basic Information** area, set the following mandatory parameters. Retain the default values for other parameters.

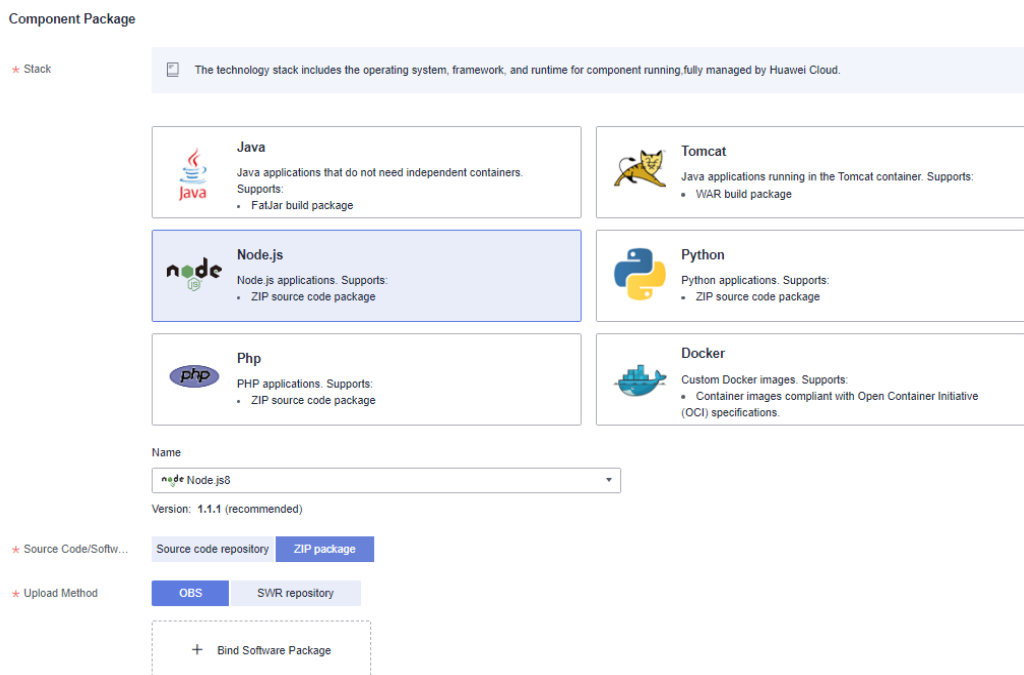
Parameter	Description
Component Name	Enter the frontend component name weathermapweb .
Component Version	Click Generate . By default, the version number is generated based on the time when you click Generate . The format is yyyy.mmdd.hhmms , in which s is the ones digit of second in the timestamp. For example, if the timestamp is 2022.0803.104321, the version number is 2022.0803.10431.

Parameter	Description
Environment	Select the environment created in Creating an Environment , for example, env-test .
Application	Select the application created in Creating an Application , for example, weathermap .

Step 4 In the **Component Package** area, set the following mandatory parameters. Retain the default values for other parameters.

Parameter	Description
Stack	Select Node.js .
Upload Method	Click Select Software Package and select the uploaded software package of component weathermapweb by referring to Table 1-2 .

Figure 1-16 Setting frontend software package parameters



Step 5 In the **Build Job** area, set the following mandatory parameters. Retain the default values for other parameters.

Parameter	Description
Organization	An organization is used to manage images generated during component building. Select the organization created in Creating an Organization .

Parameter	Description
Environment	Select Use current environment to use the CCE cluster in the deployment environment to which the component belongs to build an image. In the current environment, masters and nodes in the CCE cluster must have the same CPU architecture. Otherwise, the component build fails.

Step 6 Click **Next**.

Step 7 In the **Resources** area, retain the default settings.

Step 8 In the **Access Mode** area, retain the default settings.

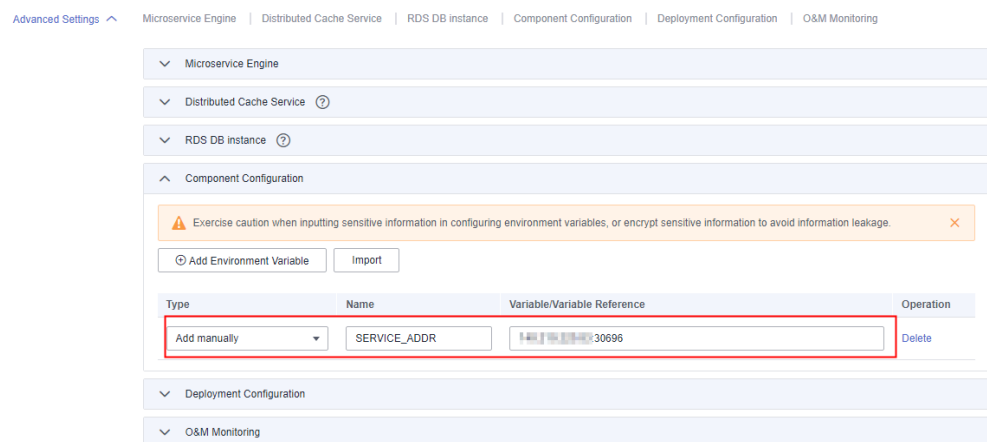
Step 9 In the **Local Time** area, retain the default settings.

Step 10 Add environment variables.

1. In the **Advanced Settings** area, expand **Component Configuration**.
2. Click **Add Environment Variable** to configure environment variables.

Type	Name	Variable/Variable Reference
Add manually	SERVICE_ADDR	Access address generated in Setting the Access Mode of the edge-service Component .


Figure 1-17 Adding environment variables



Step 11 Click **Create and Deploy**.

----End

Confirming the Deployment Result

- Step 1** Click  in the upper left corner to return to the **Application Management** page.
- Step 2** Choose **Cloud Service Engine > Microservice Catalog**.
- Step 3** Select the microservice engine where the microservice application is deployed from the **Microservice Engine** drop-down list.
- Step 4** On the **Microservice List** tab, select **weathermap** from the **All applications** drop-down list.

If the number of instances of each microservice is the same as listed in the following table, the deployment is successful.

Component Name	Instances
weather	2
forecast	1
fusionweather	1
edge-service	1

----End

Setting the Access Mode

- Step 1** Choose **Application Management**.
- Step 2** Click the application created in [Creating an Application](#) (for example, **weathermap**). The **Overview** page is displayed.
- Step 3** In the **Component List** area, locate the row that contains **weathermapweb** and click **View Access Mode** in the **External Access Address** column.
- Step 4** Click **Add Service** in the **TCP/UDP Route Configuration** area and set parameters by referring to the following table.

Parameter	Description
Service Name	Retain the default value.
Access Mode	Select Public network access .
Access Type	Select Elastic IP address .
Service Affinity	Retain the default value.
Protocol	Select TCP .
Container Port	Enter 3000 .
Access Port	Select Automatically generated .

Figure 1-18 Setting the access mode

✕

Add Service

* Service name

Access Mode Intra-cluster access Intra-VPC access Public network access
Allows access from the Internet over TCP/UDP, including EIP.

* Access Type

Container Port Cluster level Node level
 1. All nodes in the cluster can use their IP addresses+port numbers to access the workload targeted by the service.
 2. Routing hops will be used. As a result, routing performance will be compromised and clients' source IP addresses will be masked.

* Port Mapping

Protocol	Container Port	Access Port
TCP	3000	Automatically ...

Step 5 Click **OK**.

Figure 1-19 Access address

TCP/UDP Route Configuration Supports Layer-4 TCP/UDP load balancing

Internal Domain Name Access Address	Access Address	Access Mode	Protocol	Container Port	Access Port	Operation
weathermapweb.default.svc.cluster.local:3000	<input type="text" value="弹性公网IP:32314"/>	Public network access → EIP	TCP	3000	32314	Edit Delete

----End

Accessing an Application

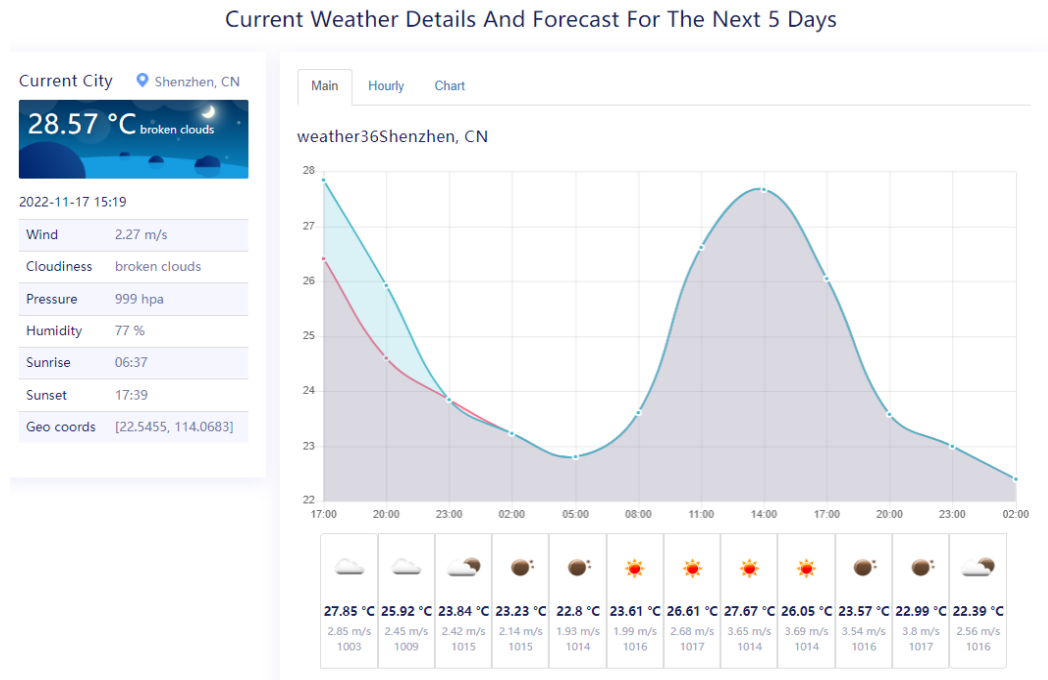
Step 1 Click in the upper left corner to return to the **Application Management** page.

Step 2 Click the application created in [Creating an Application](#) (for example, **weathermap**). The **Overview** page is displayed.

Step 3 In the **Component List** area, locate the row that contains **weathermapweb** and click **View Access Mode** in the **External Access Address** column.

If the following page is displayed, the weather forecast microservice application is successfully deployed.

Figure 1-20 Application deployed successfully



NOTE

- The data is real-time data.
- When you access the application for the first time, it takes some time for the weather system to be ready. If the preceding page is not displayed, refresh the page.

----End

1.4 Microservice Routine O&M

Scenarios

ServiceStage supports application monitoring, events, alarms, logs, tracing diagnosis, and built-in AI capabilities, implementing easy O&M.

User Story

In actual application scenarios, you can monitor application running status in real time based on graphic metrics and threshold-crossing alarms. In addition, you can quickly locate application running problems and analyze performance bottlenecks based on performance management and log policies.

Procedure

- Step 1** Log in to ServiceStage.
- Step 2** Choose **Application Management**.
- Step 3** Click an application (for example, **weathermap**). The **Overview** page is displayed.

Step 4 In the **Component List** area, click the target component. The component overview page is displayed.

Perform routine O&M by referring to [Component O&M](#).

----End

1.5 Dark Launch

The weather-beta microservice is a new version of the weather microservice and allows you to query the UV index. Before upgrading to weather-beta, a small number of requests are diverted to the later version for function verification. If the functions are normal, the earlier version will be brought offline. During the upgrade, customer requests should not be interrupted. During the deployment of the later version, traffic is not diverted to the later version. Before the earlier version is brought offline, traffic is migrated from the earlier version to the later version.

ServiceStage provides dark launch to achieve the preceding objectives.

This section describes how to deploy weather-beta using dark launch of ServiceStage.

Step 1 Log in to ServiceStage.

Step 2 Choose **Application Management**.

Step 3 Click an application (for example, **weathermap**). The **Overview** page is displayed.

Step 4 In the **Component List** area, click the target weather component. The component overview page is displayed.

Step 5 In the upper right corner of the page, click **Upgrade**.


Step 6 Select **Dark Launch (Canary)** and click **Next**.

Step 7 Configure the dark launch version based on how you deploy the weather forecast microservice.

- If **source code** is used for deployment, set the following mandatory parameters. Retain the default values for other parameters.

Parameter	Description
Command	Select Default command or script .
Dockerfile Address	Enter ./weather-beta/
Component Version	Click Generate . By default, the version number is generated based on the time when you click Generate . The format is yyyy.mmdd.hhmmss , in which s is the ones digit of second in the timestamp. For example, if the timestamp is 2022.0803.104321, the version number is 2022.0803.10431.

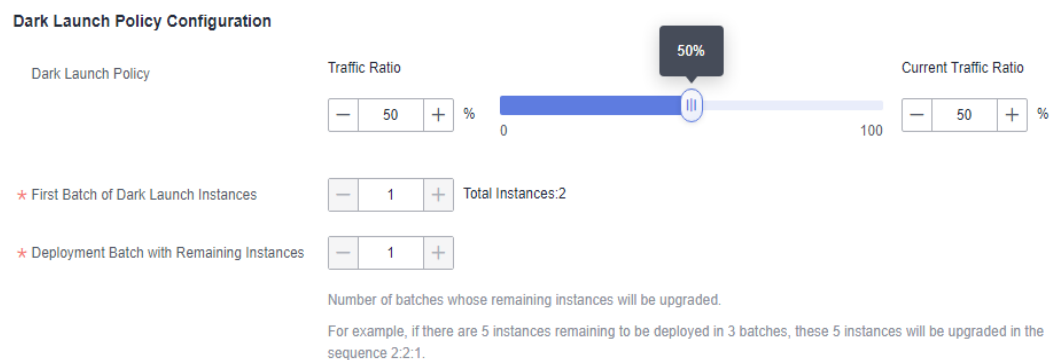
- If a **software package** is used for deployment, set the following mandatory parameters. Retain the default values for other parameters.

Parameter	Description
Upload Method	Move the cursor to the name of the weather-1.0.0.jar software package, click  , and select the weather-beta-2.0.0.jar software package uploaded in Downloading and Uploading Component Software Packages .
Component Version	Click Generate . By default, the version number is generated based on the time when you click Generate . The format is yyyy.mmdd.hhmmss , in which s is the ones digit of second in the timestamp. For example, if the timestamp is 2022.0803.104321, the version number is 2022.0803.10431.

Step 8 Configure the dark launch policy by referring to the following table.

Parameter	Description
Dark Launch Policy	<ul style="list-style-type: none"> • Traffic Ratio: set this parameter to 50%. • Current Traffic Ratio: automatically adjusted to 50%.
First Batch of Dark Launch Instances	Set this parameter to 1 .
Deployment Batch with Remaining Instances	Set this parameter to 1 .

Figure 1-21 Configuring the dark launch policy



Step 9 Click **Upgrade**.

Wait until the component status changes from **Upgrading/Rolling back the component** to **Releasing**, indicating that the component is released in dark launch.

After the dark launch is successful, the `servicecomb.routeRule.weather` configuration item is delivered to the microservice engine connected to the weather microservice.

You can view the configuration item from **Cloud Service Engine > Configuration Management**.

Step 10 Ensure that the dark launch version is working properly.

Access the application by referring to [Accessing an Application](#) and refresh the weather forecast page multiple times. The pages of the dark launch version and of the current version are periodically displayed based on the dark launch policy.

Figure 1-22 Current version (without UV data)

Current Weather Details And Forecast For The Next 5 Days

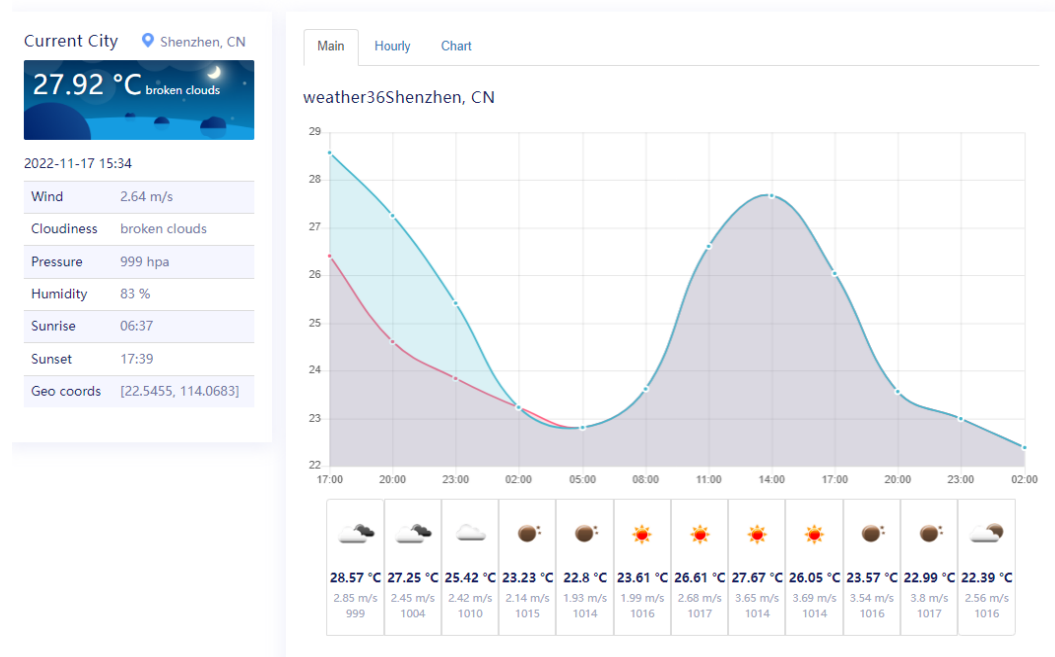


Figure 1-23 Dark launch version (with UV data)

Current Weather Details And Forecast For The Next 5 Days



----End

1.6 Microservice Governance

Scenarios

Microservice engines provide governance policies such as load balancing, service degradation, rate limiting, fault tolerance, circuit breaker, fault injection, blacklist, and whitelist.

User Story

You can configure governance policies in advance based on actual service scenarios to flexibly respond to service requirement changes and ensure stable running of applications.

Service degradation: In this practice, if the number of frontend requests increases sharply, the system responds slowly or may even break down. In this case, you can degrade the forecast microservice from fusionweather and request only important real-time weather data to ensure the proper running of important service functions and restore the service when traffic peaks are over.

Service Degradation

ServiceStage supports service degradation by microservice or API. The following uses the forecast microservice as an example.

Step 1 Log in to ServiceStage.

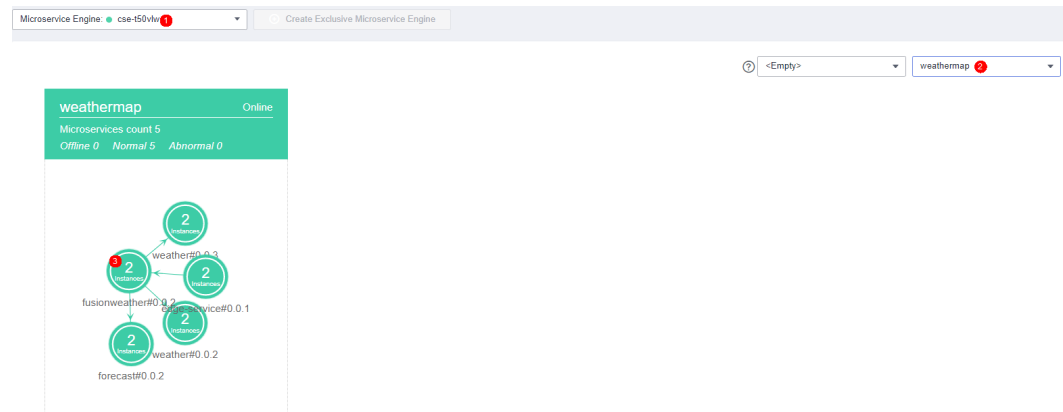
Step 2 Choose **Cloud Service Engine > Microservice Governance**.

Step 3 Select the microservice engine where the weather forecast component is deployed from the **Microservice Engine** drop-down list.

Step 4 Select **weathermap** from the **All applications** drop-down list.

Step 5 Click the **fusionweather** microservice. The **Microservice Governance** page is displayed.

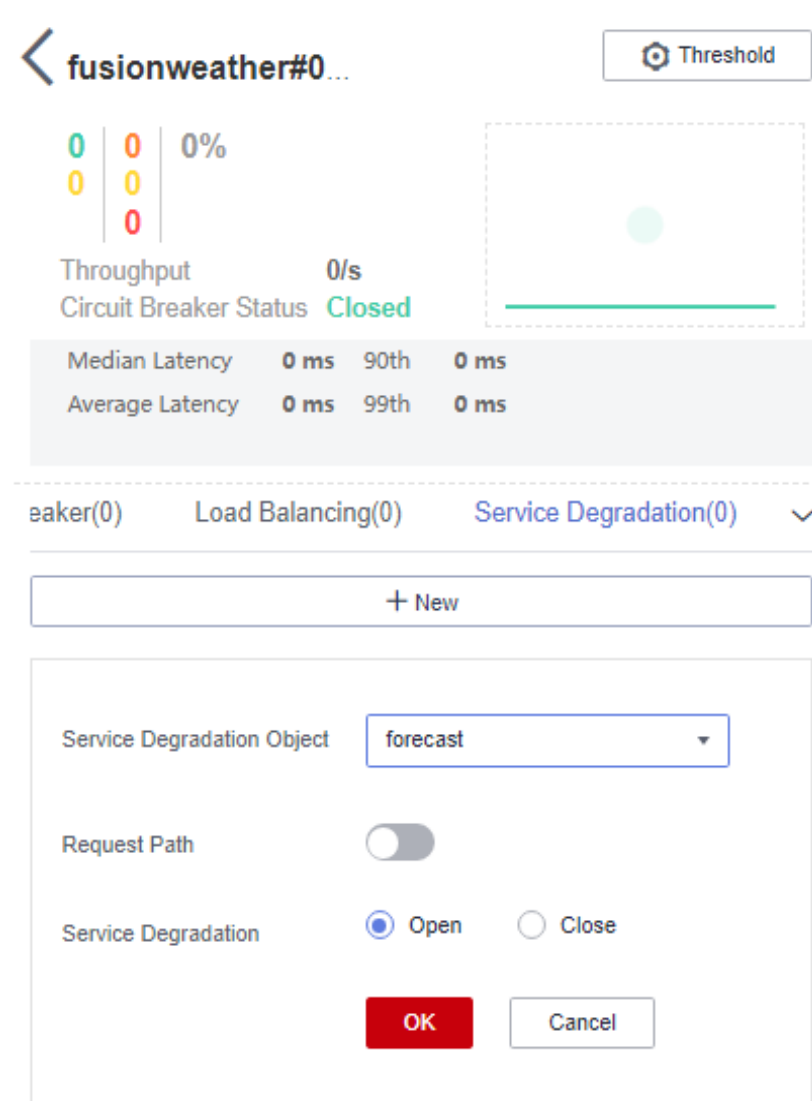
Figure 1-24 Accessing the Microservice Governance page



Step 6 Set a service degradation policy.

1. Select **Service Degradation**.
2. Click **New**.
3. Set **Service Degradation Object** to **forecast**.
4. Disable **Request Path**.
5. Set **Service Degradation** to **Open**.
6. Click **OK**.

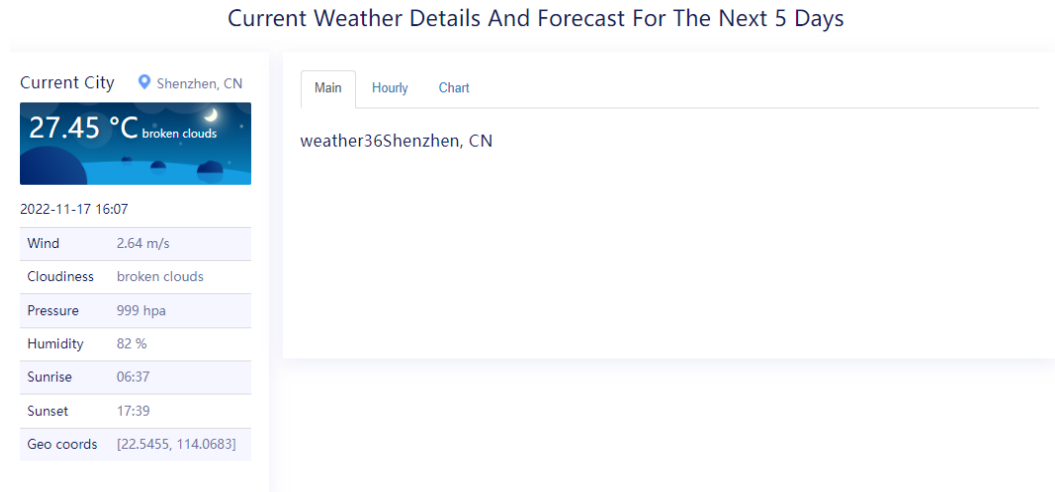
Figure 1-25 Setting a service degradation policy



Step 7 Check the configurations.

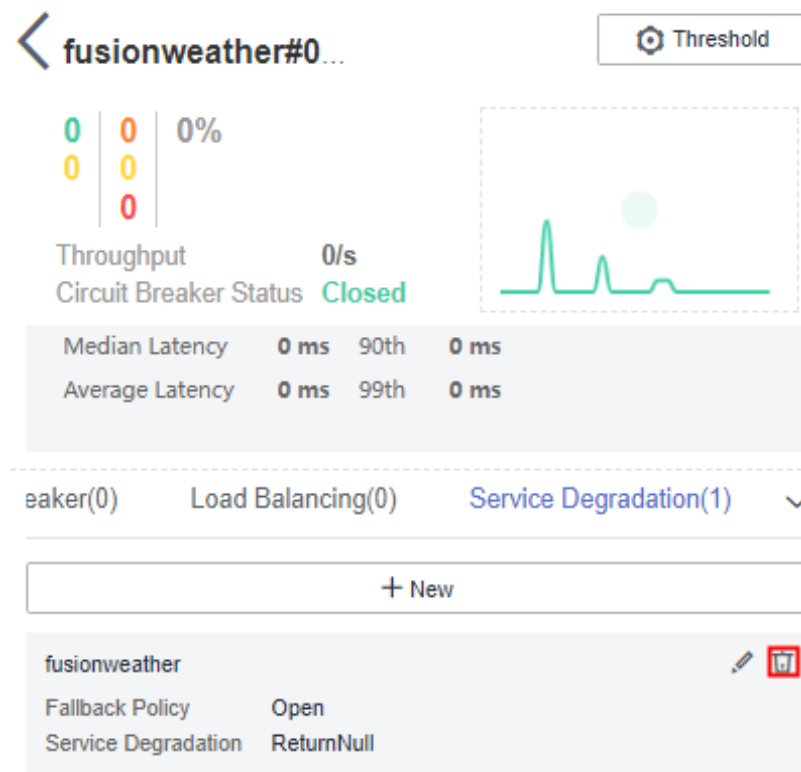
Access the application. The weather forecast on the right is blank.

Figure 1-26 Microservice degraded



Step 8 Click to delete the service degradation policy to prevent it from affecting user experience.

Figure 1-27 Deleting a policy



----End

1.7 FAQs

1.7.1 What Should I Do If a Weather Forecast Application with the Same Name Exists in the Current Environment?

Symptom

When you create a weather forecast application with a specified name (for example, **weathermap**) on ServiceStage, the system displays the error "SVCSTG.00100458: The application name already exists" indicating that an application with the same name exists in the application list.

Solution

- Step 1** When creating an application, set **Name** to a unique application name, for example, **weathermap_test**.
- Step 2** Click the created weather forecast application, for example, **weathermap_test**. The application **Overview** page is displayed.
- Step 3** Click **Environment Variables** and select an environment (for example, **env-test**) from the drop-down list.
- Step 4** Click **Add Environment Variable** to configure environment variables.
 1. Set **Name** based on the selected source code repository branch by referring to the following table.

Technology Used by Microservice Components	Name
Java Chassis	servicecomb_service_application
Spring Cloud	spring_cloud_servicecomb_discovery_appName

2. Set **Variable/Variable Reference** to the name of the created application, for example, **weathermap_test**.

- Step 5** Click **Submit**.

----End

2 Enabling Security Authentication for an Exclusive Microservice Engine

Overview

The exclusive microservice engine supports security authentication based on the Role-Based Access Control (RBAC) policy and allows you to enable or disable security authentication.

After security authentication is enabled for an engine, the security authentication account and password must be configured for all microservices connected to the engine. Otherwise, the microservice fails to be registered, causing service loss.

Application Scenarios

This section describes how to enable security authentication for an exclusive microservice engine and ensure that services of microservice components connected to the engine are not affected.

Procedure

Step 1 Upgrade the SDK used by microservice components.

To enable the security authentication function, SDK must support the security authentication function. If the SDK version used by the current microservice components is earlier than the required version (Spring Cloud Huawei requires 1.6.1 or later, and Java chassis requires 2.3.5 or later), you need to upgrade SDK.

Step 2 Configure security authentication parameters for microservice components.

Before enabling security authentication for a microservice engine, configure security authentication parameters for the microservice components that have been connected to the engine. To configure security authentication parameters, you need to configure the security authentication account and password:

- Configuring the security authentication account and password for a Spring Cloud microservice component

Table 2-1 Configuring the security authentication account and password for a Spring Cloud microservice component

Configuration File Configuration	Environmental Variables Injection
<p>Add the following configurations to the bootstrap.yml file of the microservice. If they are configured, skip this step.</p> <pre> spring: cloud: servicecomb: credentials: account: name: test #Security authentication account. Set this parameter based on the site requirements. password: mima #Password of the security authentication account. Set this parameter based on the site requirements. cipher: default </pre>	<p>Add the following environment variables. For details, see Managing Application Environment Variables.</p> <ul style="list-style-type: none"> • <code>spring_cloud_servicecomb_credentials_account_name</code>: security authentication account. Set this parameter based on the site requirements. • <code>spring_cloud_servicecomb_credentials_account_password</code>: password of the security authentication account. Set this parameter based on the site requirements.

 **NOTE**

- By default, the user password is stored in plaintext, which cannot ensure security. You are advised to encrypt the password for storage. For details, see [Custom Encryption Algorithms for Storage](#).
- If security authentication is not enabled for the microservice engine and security authentication parameters are configured for the microservice components connected to the microservice engine, the normal service functions of the microservice components are not affected.
- Configuring the security authentication account and password for a Java Chassis microservice component

Table 2-2 Configuring the security authentication account and password for a Java Chassis microservice component

Configuration File Configuration	Environmental Variables Injection
<p>Add the following configurations to the microservice.yml file of the microservice. If they are configured, skip this step.</p> <pre> servicecomb: credentials: rbac.enabled: true #Whether to enable security authentication. Set this parameter based on the site requirements. cipher: default account: name: test #Security authentication account. Set this parameter based on the site requirements. password: mima #Password of the security authentication account. Set this parameter based on the site requirements. cipher: default </pre>	<p>Add the following environment variables. For details, see Managing Application Environment Variables.</p> <ul style="list-style-type: none"> - servicecomb_credentials_rbac_enabled: whether to enable security authentication. Set this parameter based on the site requirements. true: security authentication is enabled; false: security authentication is disabled. - servicecomb_credentials_account_name: security authentication account. Set this parameter based on the site requirements. - servicecomb_credentials_account_password: password of the security authentication account. Set this parameter based on the site requirements.

Step 3 Enable security authentication for an exclusive microservice engine. For details, see [Enabling Security Authentication](#).

 **NOTE**

After security authentication is 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.

----End

3 Connecting Microservice Engine Dashboard Data to AOM through ServiceStage

Background

The real-time monitoring data of a Java chassis application deployed on the microservice engine dashboard is retained for 5 minutes by default. To permanently store historical monitoring data for subsequent query and analysis, use the custom metric monitoring function of ServiceStage to connect the microservice data displayed on the microservice engine dashboard to AOM.

This section uses the application deployed using a software package as an example to describe how to complete the connection.

Procedure

Step 1 Add dependency.

In the development environment, open the application project that requires persistent storage of historical monitoring data and add the following dependency to the **pom** file of the microservice:

```
<dependency>
  <groupId>org.apache.servicecomb</groupId>
  <artifactId>metrics-core</artifactId>
</dependency>
<dependency>
  <groupId>org.apache.servicecomb</groupId>
  <artifactId>metrics-prometheus</artifactId>
</dependency>
```

Step 2 Recompile and package the application project to which the dependency has been added, and upload the package.

- Upload the software package to the SWR software repository. For details, see [Uploading the Software Package](#) .
- Upload the software package to the OBS bucket. For details, see [Uploading an Object](#).

Step 3 Deploy the application component.

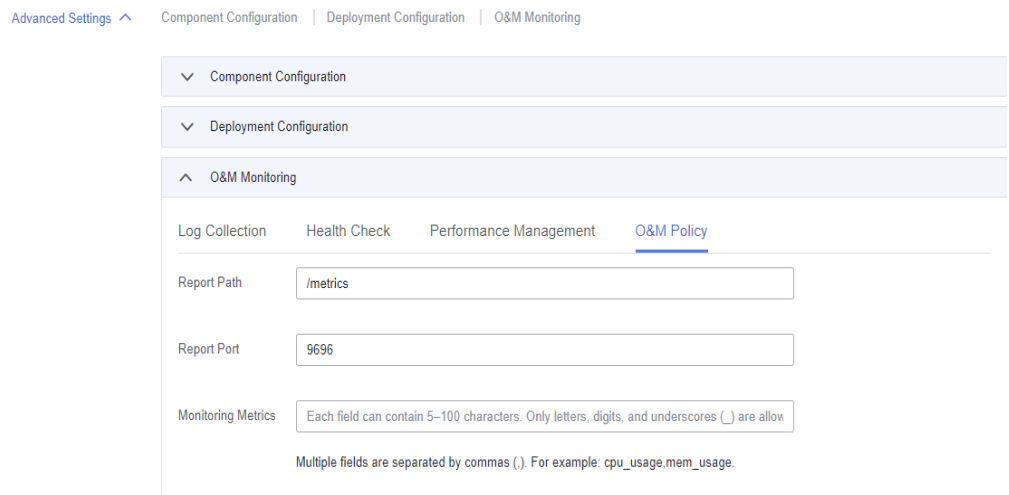
- To deploy a new component, go to **Step 4**.
- If the component has been deployed, go to **Step 5**.

Step 4 Deploy the component that is packaged and uploaded in **Step 2**. For details, see **Creating and Deploying Components**.

1. During component deployment, choose **Advanced Settings > O&M Monitoring > O&M Policy** and configure the following parameters:

Parameter	Value
Report Path	/metrics
Report Port	9696

Figure 3-1 Setting custom monitoring



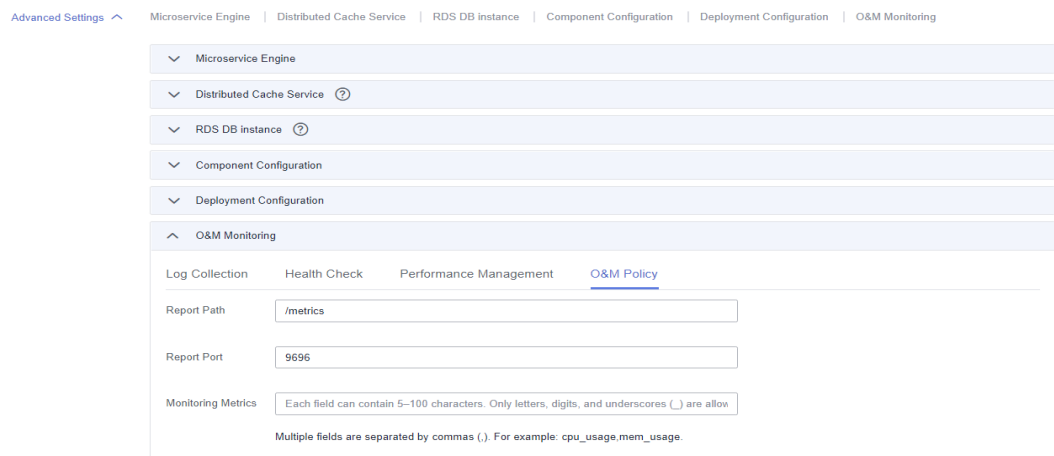
2. After the component is successfully deployed, go to **Step 6**.

Step 5 Connect monitoring metrics to AOM.

1. Log in to ServiceStage.
2. Choose **Application Management**.
3. Click the application where the component is located. The **Overview** page of the application is displayed.
4. In the **Component List** area, click the target component. The component overview page is displayed.
5. Click **Deploy**.
6. Select **Single-batch Release** and click **Next**.
7. Choose **Advanced Settings > O&M Monitoring > O&M Policy** and configure the following parameters:

Parameter	Value
Report Path	/metrics
Report Port	9696

Figure 3-2 Monitoring metrics



8. Click **Deploy** and wait until the component is redeployed successfully.

Step 6 On the AOM console, view monitoring metrics and export monitoring data. For details, see [Metric Monitoring](#).

----End

4 Migrating the Registered Microservice Engine Using ServiceStage Without Code Modification

Context

This section describes how to migrate the microservice application components that are developed using the Java chassis microservice framework and registered with the professional microservice engine to the exclusive microservice engine without any code modification.

NOTICE

Services will be interrupted during the migration of the microservice registration engine. Evaluate and select a proper time window before the migration.

Prerequisites

You have created an exclusive microservice engine with security authentication disabled. For details, see [Creating a Microservice Engine](#).

Select the VPC in the microservice application component environment the same as the VPC and subnet where the engine is located.

Procedure


Step 1 Log in to ServiceStage.

Step 2 Delete the deployed microservice application component instances.

1. Choose **Application Management**.
2. Click the application where the microservice application is located. The **Overview** page is displayed.
3. In the **Component List** area, select the components to be deleted and click **Bulk Delete**.

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

Step 3 Modify the environment for deploying microservice application components.

1. Click  in the upper left corner to return to the **Application Management** page.
2. Choose **Environment Management**.
3. Click the environment where the microservice application is deployed.
4. In the **Resource Settings** area, choose **Cloud Service Engine** from **Middleware**.
5. Select **Cloud Service Engine** and click **Remove**.
6. Click **Manage Resource**.
7. Select the created exclusive microservice engine and click **OK**.

Step 4 Deploy the application instance. For details, see [Creating and Deploying Components](#).

----End

5 Hosting a Spring Boot Application on ServiceStage

5.1 Preparations

Spring Boot is an open-source application development framework based on the Spring framework. It helps you quickly build stand-alone and production ready applications.

This best practice uses the sample code provided by Spring to help you quickly deploy, access, and upgrade Spring applications on ServiceStage.

Preparing Required Resources

To facilitate subsequent operations, ensure that:

1. You have created a VPC. For details, see [Creating a VPC](#).
2. You have created a Cloud Container Engine (CCE) cluster. In a trial scenario, set **Management Scale** to **50 nodes** and **HA** to **No**.

The cluster contains at least one ECS node with 8 vCPUs and 16 GB memory or two ECS nodes with 4 vCPUs and 8 GB memory, and is bound to an EIP. For details, see [Buying a Cluster](#).

- The VPC to which the CCE cluster belongs is the one created in **1**.
 - If you have [enabled the enterprise project function](#), the CCE cluster and its VPC must be in the same enterprise project.
 - The CCE cluster cannot be bound to other environments.
 - If a CCE cluster 1.23 or later is created, **Container Engine** of the ECS node in the cluster supports only Docker.
3. You have registered and obtained a public domain name from the domain name provider. For details, see [Creating a Public Zone](#).
 4. In this example, the GitHub source code repository is bound to ServiceStage to implement source code building, archiving, and application creation. Ensure that you have registered an account on [GitHub](#).

Forking the Source Code

Use your account to log in to GitHub and fork the official Spring Boot source code of the baseline version and dark launch version to your GitHub repository.

1. Address for source code of the baseline version: <https://github.com/spring-guides/gs-spring-boot/tree/boot-2.7>
2. Source code address of the dark launch version: <https://github.com/herocc19/gs-spring-boot-kubernetes>

Setting GitHub Repository Authorization

You can set GitHub repository authorization so that build projects and application components can use the authorization information to access the GitHub source code repository.

Step 1 Log in to ServiceStage.

Step 2 Choose **Continuous Delivery > Repository Authorization > Create Authorization** and configure authorization information by referring to the following table. Parameters marked with an asterisk (*) are mandatory.

Table 5-1 Authorization information

Parameter	Description
*Name	Use the default authorization name. This name cannot be changed after being created.
*Repository Type	<ol style="list-style-type: none">1. Select GitHub.2. Select an authorization method.<ul style="list-style-type: none">– OAuth: Click Use OAuth Authorization and complete the authorization creation as prompted.– Personal token: Enter the obtained private token and click Create.

Step 3 Click **Create**.

----End

Creating an Organization

Step 1 Choose **Deployment Source Management > Organization Management**.

Step 2 Click **Create Organization**. On the displayed page, specify **Organization Name**. For example, **org-test**.

Step 3 Click **OK**.

Figure 5-1 Creating an organization

Create Organization

- Each organization name must be globally unique.
- The current account can create a maximum of 5 organizations.
- For centralized management of images, limit each organization to one company, department, or individual.

Example:

Company or department: cloud-hangzhou or cloud-develop

Person: john

* Organization Name

----End

Creating an Environment

Step 1 Choose **Environment Management > Create Environment** and set the environment information by referring to the following table.

Parameter	Description
Environment	Enter an environment name, for example, env-test .
Enterprise Project	Specify Enterprise Project . Enterprise projects let you manage cloud resources and users by project. It is available after you enable the enterprise project function . The environment and its VPC must be in the same enterprise project.
Description	Retain the default value.
VPC	Select the VPC prepared in Preparing Required Resources . NOTE The VPC cannot be modified after the environment is created.
Environment Type	Select Kubernetes .

Figure 5-2 Configuring an environment

The screenshot displays the configuration interface for creating an environment. It includes the following elements:

- Environment:** A text input field containing "env-test".
- Enterprise Project:** A dropdown menu showing "default" and a "Create Enterprise Project" button.
- Description:** A field with a placeholder "--" and an edit icon.
- VPC:** A dropdown menu showing "vpc-test" and a "Create a VPC" button.
- Environment Type:** Two buttons: "VM" and "Kubernetes", with "Kubernetes" selected.


Step 2 Click **Create Now**.

Step 3 In the **Resource Settings** area, choose **Cloud Container Engine** from **Compute** and click **Bind now**.

Step 4 In the dialog box that is displayed, select the CCE cluster created in [Preparing Required Resources](#) and click **OK**.

----End

Creating an Application

Step 1 Click  in the upper left corner to return to the **Environment Management** page.

Step 2 Choose **Application Management > Create Application** and set basic application information.

1. **Name:** Enter an application name, for example, **springGuides**.
2. **Enterprise Project:** Enterprise projects let you manage cloud resources and users by project.

It is available after you [enable the enterprise project function](#). The application and [its environment](#) must be in the same enterprise project.

Step 3 Click **OK**.

Figure 5-3 Creating an application

Create Application

----End

5.2 Deploying and Accessing Spring Boot Applications

To deploy and access Spring Boot applications, perform the following steps:

1. [Creating and Deploying Spring Boot Application Components](#)
2. [Accessing Spring Boot Applications](#)

Creating and Deploying Spring Boot Application Components

- Step 1** Log in to ServiceStage.
- Step 2** Choose **Application Management**. The application list is displayed.
- Step 3** Click **Create Component** in the **Operation** column of the application created in [Creating an Application](#) (for example, **springGuides**).
- Step 4** In the **Basic Information** area, set the following mandatory parameters. Retain the default values for other parameters.

Parameter	Description
Component Name	Enter a component name, for example, spring-boot .
Component Version	Enter 1.0.0 .
Environment	Select the environment created in Creating an Environment , for example, env-test .
Application	Select the application created in Creating an Application , for example, springGuides .

Figure 5-4 Setting the basic component information


Basic Information

* Component Name

* Component Version

* Environment

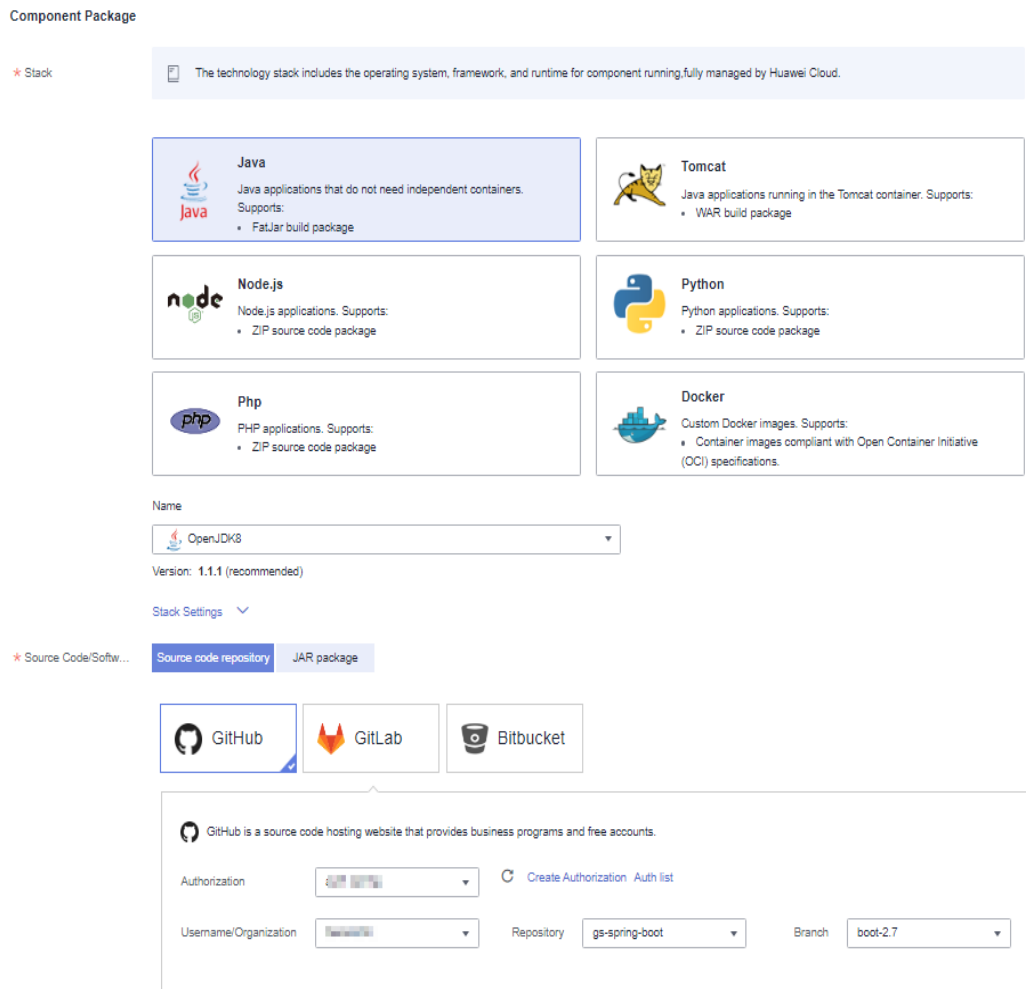
* Application

Description -- 

Step 5 In the **Component Package** area, set the following mandatory parameters. Retain the default values for other parameters.

Parameter	Description
Stack	Select Java .
Source Code/ Software Package	<ol style="list-style-type: none"> 1. Select Source code repository. 2. Select GitHub, 3. Authorization: Select the authorization information created in Setting GitHub Repository Authorization. 4. Username/Organization: Select the username used to log in to GitHub in Forking the Source Code. 5. Repository: Select the name of the Spring Boot source code repository that has been forked to your GitHub account. For example, gs-spring-boot. 6. Branch: Select boot-2.7.

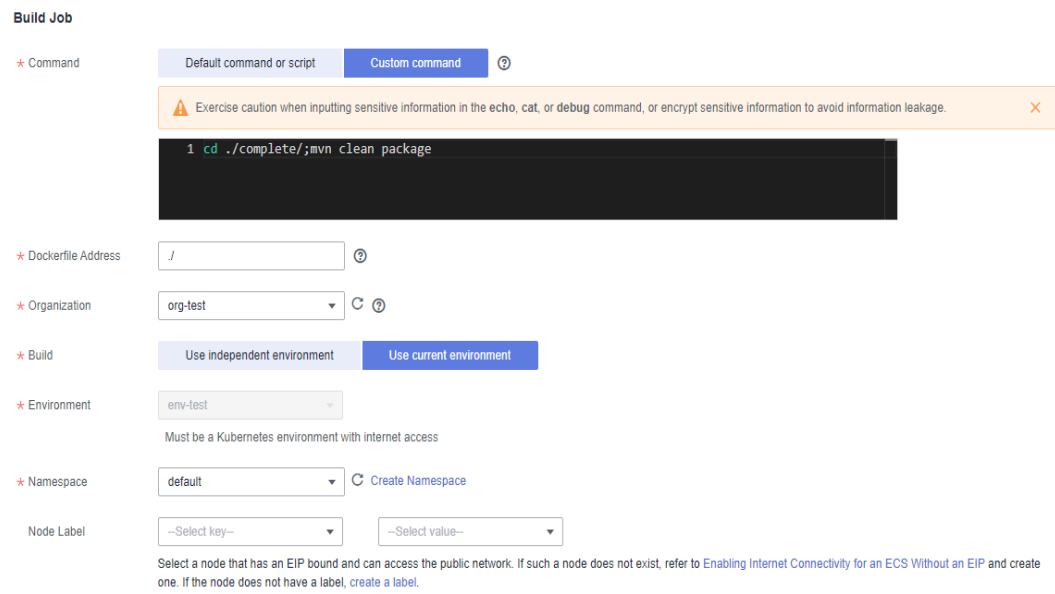
Figure 5-5 Setting software package parameters



Step 6 In the **Build Job** area, set the following mandatory parameters. Retain the default values for other parameters.


Parameter	Description
Command	<ol style="list-style-type: none"> 1. Select Custom command. 2. Enter the following command in the command text box: <code>cd ./complete;/mvn clean package</code>
Organization	Select the organization created in Creating an Organization . An organization is used to manage images generated during component building.
Environment	<p>Select Use current environment to use the CCE cluster in the deployment environment to which the component belongs to build an image.</p> <p>In the current environment, masters and nodes in the CCE cluster must have the same CPU architecture. Otherwise, the component build fails.</p>

Figure 5-6 Configuring build parameters



Step 7 Click **Next**.

Step 8 In the **Resources** area, retain the default settings.

Step 9 In the **Access Mode** area, click  to enable **Public Network Access** and set public network access parameters for the component by referring to the following table.

Parameter	Description
Public Network Access	Enable this option.
Public Network Load Balancer	By default, managed ELBs in the deployment environment to which the component belongs are selected.
Client Protocol	Retain the default value.
Domain Name	Select Bind Domain Name and enter the public domain name obtained in Preparing Required Resources .
Listening Port	Enter 8080 .


Step 10 In the **Local Time** area, retain the default settings.

Step 11 In the **Advanced Settings** area, retain the default settings.

Step 12 Click **Create and Deploy**.

----End

Accessing Spring Boot Applications

- Step 1** Click  in the upper left corner to return to the **Application Management** page.
- Step 2** Click the application created in [Creating an Application](#) (for example, **springGuides**). The **Overview** page is displayed.
- Step 3** In the **Component List** area, locate the row that contains the component name (for example, **spring-boot**) configured in [Creating and Deploying Spring Boot Application Components](#) and click the access address in the **External Access Address** column to access the application.

If information similar to the following is displayed, the application is successfully deployed:

Greetings from Spring Boot!

----End

5.3 Upgrading Component Versions Using ELB Dark Launch

- Step 1** Go to the ServiceStage console.
- Step 2** Choose **Application Management**. The application list is displayed.
- Step 3** Click the application created in [Creating an Application](#) (for example, **springGuides**). The **Overview** page is displayed.
- Step 4** On the **Component List** tab, click the component created in [Deploying and Accessing Spring Boot Applications](#) (for example, **spring-boot**). The **Overview** page is displayed.
- Step 5** In the upper right corner of the page, click **Upgrade**.
- Step 6** Set **Upgrade Type** to **Dark Launch (Canary)** and click **Next**.
- Step 7** Set mandatory parameters for dark launch by referring to the following table. Retain the default values for other parameters.

Parameter	Description
Source Code/Image	<p>The value is fixed to the GitHub source code repository selected during component creation and deployment.</p> <ol style="list-style-type: none"> 1. Click Modify. 2. Authorization: Select the authorization information created in Setting GitHub Repository Authorization. 3. Username/Organization: Select the username used to log in to GitHub in Forking the Source Code. 4. Repository: Select the name of the Spring Boot source code repository that has been forked to your GitHub account. For example, gs-spring-boot-kubernetes. 5. Branch: Select main.

Parameter	Description
Command	<ol style="list-style-type: none"> 1. Select Custom command. 2. Enter the following command in the command text box: <code>cd ./complete;/mvn clean package</code>
Component Version	Enter 1.0.1 .
Dark Launch Policy	<ul style="list-style-type: none"> • Traffic Ratio: Percentage of traffic directed to the new version. Set this parameter to 50. • Current Traffic Ratio : Percentage of traffic directed to the current version. The value is automatically set to 50.
First Batch of Dark Launch Instances	Set this parameter to 1 .
Deployment Batch with Remaining Instances	Set this parameter to 1 .

Step 8 Click **Upgrade**.

Wait until the component status changes from **Upgrading/Rolling back the component** to **Releasing**, indicating that the component is released in dark launch.

Step 9 Perform **Accessing Spring Boot Applications** multiple times. If "Greetings from Spring Boot!" and "Hello" are displayed alternately on the page, the dark launch version of ELB is released.

----End

6 Using GitLab to Interconnect with Jenkins to Automatically Build and Upgrade Components Deployed on ServiceStage

6.1 Overview

After the code is developed, you need to pack the code into an image package or JAR package on Jenkins before each rollout, upload the image package to SWR or the JAR package to OBS, and then use ServiceStage to upgrade the component version. This process is complex. Frequent version tests cause low development and O&M efficiency and poor user experience.

If you manage your code on GitLab and use ServiceStage with components deployed to host applications, you can use GitLab to interconnect with Jenkins for automatic build and packaging to upgrade the components deployed on ServiceStage.

This practice uses the shell script output after Jenkins build and packaging to automatically build and package code after integration and upgrade components deployed on ServiceStage.

6.2 Preparations

6.2.1 Preparing the Jenkins Environment

Environment Description

Install Jenkins on a Linux VM. The following lists the environment information used in this practice. If you use an image package for deployment, install Docker on the VM.

- VM: CentOS 7.9
- Jenkins: 2.319.3

- Git: installed using yum
- JDK: 11.0.8
- Apache Maven: 3.8.6

NOTE

The following parameter needs to be added to start Jenkins:

```
-Dhudson.security.csrf.GlobalCrumbIssuerConfiguration.DISABLE_CSRF_PROTECTION=true
```

Otherwise, GitLab fails to interconnect with Jenkins. The error is as follows:

```
HTTP Status 403 - No valid crumb was included in the request
```

Downloading and Installing Related Software

- Download and install Jenkins.
Download: <https://mirrors.jenkins.io/war-stable/>. Install: <https://www.jenkins.io/doc/book/installing/>.
- Install Git to pull code for building commands.

```
yum install git -y
```
- Download JDK.
<https://www.oracle.com/java/technologies/downloads/#java11>
- Download Maven.
<https://maven.apache.org/download.cgi>
- Install Docker to pack the image package and upload it to the image repository.

```
yum install docker
```

Verifying the Installation

- Git

```
[root@ecs-jenkins ~]# git version  
git version 1.8.3.1
```
- JDK

```
[root@ecs-jenkins jar]# java -version  
openjdk version "1.8.0_345"  
OpenJDK Runtime Environment (build 1.8.0_345-b01)  
OpenJDK 64-Bit Server VM (build 25.345-b01, mixed mode)
```
- Maven

```
[root@ecs-jenkins jar]# mvn -v  
Apache Maven 3.8.6 (84538c9988a25aec085021c365c560670ad80f63)  
Maven home: /root/app/maven/apache-maven-3.8.6  
Java version: 11.0.8, vendor: Huawei Technologies Co., LTD, runtime: /root/app/jdk11/jdk-11.0.8  
Default locale: en_US, platform encoding: UTF-8  
OS name: "linux", version: "3.10.0-1160.76.1.el7.x86_64", arch: "amd64", family: "unix"
```
- Docker

```
[root@ecs-jenkins jar]# docker version  
Client:  
Version:      1.13.1  
API version:  1.26  
Package version: docker-1.13.1-209.git7d71120.el7.centos.x86_64  
Go version:   go1.10.3  
Git commit:   7d71120/1.13.1  
Built:        Wed Mar 2 15:25:43 2022  
OS/Arch:     linux/amd64  
Server:  
Version:      1.13.1  
API version:  1.26 (minimum version 1.12)  
Package version: docker-1.13.1-209.git7d71120.el7.centos.x86_64
```

```
Go version: go1.10.3
Git commit: 7d71120/1.13.1
Built: Wed Mar 2 15:25:43 2022
OS/Arch: linux/amd64
Experimental: false
```

6.2.2 Uploading Code to GitLab

This practice uses Java project code and uses Maven to build JAR packages.

Prerequisites

1. The Linux VM where Jenkins is located can access the GitLab code repository.
2. An account and a repository have been created on GitLab.

Procedure

Step 1 Log in to GitLab.

Step 2 Upload code to the code repository.

----End

6.2.3 Installing and Initializing obsutil

obsutil is used to upload software packages to OBS.

Prerequisites

1. You have obtained AK/SK. For details, see [Access Keys](#).
2. You have obtained the endpoint of the region where ServiceStage is deployed. For details, see [Regions and Endpoints](#).
3. You have created a bucket in OBS in the same region as ServiceStage where the component is deployed to store software packages. For details, see [Creating a Bucket](#).

Procedure

Step 1 Log in to the Linux VM where Jenkins is installed and install obsutil. For details, see [Download and Installation](#).

NOTE

Before installing obsutil, run the following command on the Linux VM where Jenkins is located to check the VM OS type:

```
echo $HOSTTYPE
```

- If the command output is **x86_64**, download the obsutil software package for the AMD 64-bit OS.
- If the command output is **aarch64**, download the obsutil software package for the ARM 64-bit OS.

Step 2 Initialize obsutil.

```
{path}/obsutil config -i=ak -k=sk -e={endpoint}
```

Where,

- *{path}* is the obsutil installation path, for example, `/root/tools/obsutil/obsutil_linux_amd64_5.4.6`.
- *{endpoint}* is the obtained endpoint of the region where ServiceStage is deployed.

Step 3 Check whether obsutil can be used to upload files to OBS.

1. Create a test file.

```
touch test.txt
```

2. Use obsutil to upload the file.

```
/root/tools/obsutil/obsutil_linux_amd64_5.4.6/obsutil cp test.txt obs://{OBS bucket name}
```

Replace *{OBS bucket name}* with the name of the OBS bucket to be used. In this example, the bucket name is **obs-mzc**. Upload the **test.txt** file created in the current directory to the obs-mzc bucket. If the "Upload successfully" is displayed, the upload is successful.

```
[root@ecs-jenkins jar]# /root/tools/obsutil/obsutil_linux_amd64_5.4.6/obsutil cp test1.txt obs://obs-mzc
Start at 2023-07-24 06:09:53.49127587 +0000 UTC
Parallel: 5          Jobs: 5
Threshold: 50.00MB   PartSize: auto
VerifyLength: false VerifyMd5: false
CheckpointDir: /root/.obsutil_checkpoint
[-----] 100.00% 138B/s
58B/58B 622ms
Upload successfully, 58B, n/a, /root/jar/test1.txt --> obs://obs-mzc/test1.txt, cost [621], status [200],
request id [000001898684BD614014A659111ABF74]
```

----End

6.2.4 Installing and Initializing KooCLI

KooCLI is used to call ServiceStage APIs to upgrade components.

Install and initialize KooCLI to use it.

- Install KooCLI by [Method 1: Online Installation](#) or [Method 2: Using Software Package](#)
- [Initializing KooCLI](#)

Method 1: Online Installation

Step 1 Log in to the Linux VM where Jenkins is located.

Step 2 Run the following command:

```
curl -sSL https://hwcloudcli.obs.cn-north-1.myhuaweicloud.com/cli/latest/hcloud_install.sh -o ./hcloud_install.sh && bash ./hcloud_install.sh -y
```

----End

Method 2: Using Software Package

Step 1 Log in to the Linux VM where Jenkins is located and run the following command to check the VM OS type:

```
echo $HOSTTYPE
```

- If the command output is **x86_64**, the AMD 64-bit OS is used.
- If the command output is **aarch64**, the ARM 64-bit OS is used.

Step 2 Run the following command to download the software package:

- AMD

```
wget "https://hwcloudcli.obs.cn-north-1.myhuaweicloud.com/cli/latest/huaweicloud-cli-linux-amd64.tar.gz" -O huaweicloud-cli-linux-amd64.tar.gz
```
- ARM

```
wget "https://hwcloudcli.obs.cn-north-1.myhuaweicloud.com/cli/latest/huaweicloud-cli-linux-arm64.tar.gz" -O huaweicloud-cli-linux-arm64.tar.gz
```

Step 3 Run the following command to decompress the software package:

- AMD

```
tar -zxvf huaweicloud-cli-linux-amd64.tar.gz
```
- ARM

```
tar -zxvf huaweicloud-cli-linux-arm64.tar.gz
```

Step 4 Run the following command in the decompressed directory to create a soft link to the `/usr/local/bin` directory:

```
ln -s $(pwd)/hcloud /usr/local/bin/
```

Step 5 Run the following command to check whether the installation is successful:

```
hcloud version
```

If information similar to "KooCLI version: 3.4.1.1" is displayed, the installation is successful.

----End

Initializing KooCLI

Step 1 Log in to the Linux VM where Jenkins is located.

Step 2 Enter the command and press **Enter** to enter the interactive mode, and set the parameters as prompted. For details, see [Table 6-1](#).

```
hcloud configure init
```

Table 6-1 Initial configurations

Parameter	Description
Access Key ID	Mandatory. For details, see Access Keys .
Secret Access Key	Mandatory. For details, see Access Keys .
Region	Optional. Region where ServiceStage is deployed. For details, see Regions and Endpoints .

Step 3 Add configuration parameters.

The corresponding CLI upgrade command may not be found. In this case, you need to add additional configuration.

```
hcloud configure set --cli-lang=cn
```

----End

6.2.5 Installing the Jenkins Plug-in and Configuring Jenkins

Before using GitLab to interconnect with Jenkins to automatically build and deploy components on ServiceStage, install the Jenkins plug-in and configure Jenkins global parameters.

- Install the Jenkins plug-in to interconnect with Git and use scripts during build.
- Configure Jenkins global parameters for the Jenkins pipeline packaging script to interconnect with Git to pull and package code.

Procedure

Step 1 Enter **http://{IP address of the Linux VM where Jenkins is installed}:8080** in the address box of the browser to log in to Jenkins.

Step 2 Choose **Manage Jenkins > Manage Plugins**.

Step 3 Click **Available**, search for plug-ins in [Table 6-2](#), and install them.

Table 6-2 Plug-in installation description

Plug-in	Mandatory	Description
Generic Webhook Trigger Plugin	Yes	Used to interconnect to the webhook of GitLab.
GitLab Plugin	Yes	Allows GitLab to trigger Jenkins build.
Pipeline: Basic Steps	Yes	Supports pipeline script syntax.
Pipeline: Build Step	Yes	Supports pipeline script syntax.
Pipeline: Stage Step	Yes	Supports pipeline script syntax.

Step 4 Choose **Manage Jenkins > Global Tool Configuration**.

Step 5 Configure Maven.

Replace **/root/app/maven/apache-maven-3.8.6** in the example with the actual Maven installation directory.

Maven Configuration

Default settings provider

Settings file in filesystem

File path ?

/root/app/maven/apache-maven-3.8.6/conf/settings.xml

Default global settings provider

Global settings file on filesystem

File path ?

/root/app/maven/apache-maven-3.8.6/conf/settings.xml

Maven

Maven installations

Add Maven

Maven
Name

Maven

MAVEN_HOME

/usr/share/maven

Install automatically ?

Delete Maven

Step 6 Configure JDK.

Replace **/root/app/jdk11/jdk-11.0.8** in the example with the actual JDK installation directory.

JDK

JDK installations

Add JDK

JDK
Name

jdk11

JAVA_HOME

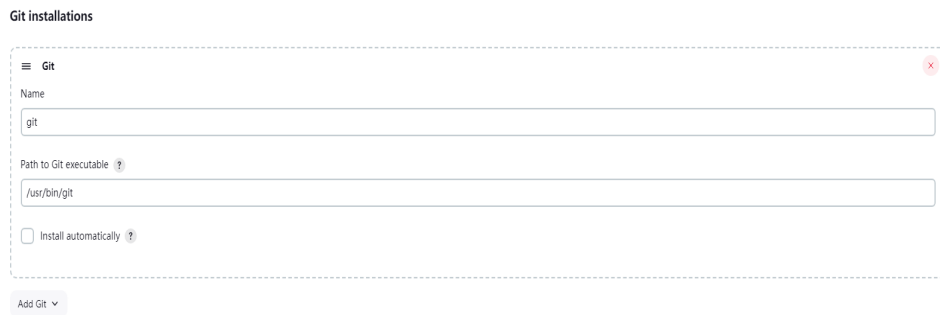
/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.382.b05-1.el7_9.x86_64/

Install automatically ?

Delete JDK

Step 7 Configure Git.

Replace **/usr/bin/git** in the example with the actual Git installation directory.



----End

6.3 Procedure

6.3.1 Interconnection Tests

Before the operation, test the interconnection between Jenkins and GitLab to ensure that Jenkins can access GitLab through APIs.

Generating a GitLab Access Token

- Step 1** Log in to GitLab.
- Step 2** Move the cursor to the account name in the upper right corner and click **Edit profile**.
- Step 3** Click **Access Tokens**, enter **Token name**, select **api**, and click **Create personal access token**.

The token will be displayed on the right of **Personal Access Tokens**.

NOTE

The token is displayed only when it is generated for the first time. Otherwise, you need to create it again next time. This token is used only for GitLab interconnection tests.

----End

Testing the Interconnection Between Jenkins and GitLab

- Step 1** Enter **http://*{IP address of the Linux VM where Jenkins is installed}*:8080** in the address box of the browser to log in to Jenkins.
- Step 2** Choose **Manage Jenkins > Jenkins Configuration**. In **Configuration**, select **Gitlab**.
- Step 3** Configure the GitLab URL, click **Add** under **Credentials**, and select **Jenkins**.
- Step 4** Select **Username with password** from the drop-down list, select **Gitlab API token**, and configure the GitLab access token in **Generating a GitLab Access Token** to the API token.

Step 5 Select **Gitlab API token** for **Credentials** and click **Test Connection**. If **Success** is displayed, the interconnection is successful.

----End

6.3.2 Configuring a Pipeline Build Task

- Scenario 1: If a software package is generated using Jenkins, for example, a JAR package, use the software package deployment scenario in the script. During deployment, the built software package is uploaded to the OBS bucket and the ServiceStage component is upgraded.
- Scenario 2: If an image package is generated using Jenkins, use the image deployment scenario in the script. During deployment, the built image package is uploaded to the SWR image repository and the ServiceStage component is upgraded.

This section uses the scenario where the instance in [Configuring a Pipeline Script](#) is a JAR package as an example.

Creating a GitLab Credential

Use the account and password with the GitLab code repository permission to create a credential in Jenkins for pulling GitLab code.

Step 1 Enter **http://*{IP address of the Linux VM where Jenkins is installed}*:8080** in the address box of the browser to log in to Jenkins.

Step 2 Choose **Manage Jenkins > Jenkins Configuration**. In **Configuration**, select **Gitlab**.

Step 3 Click **Add** under **Credentials** and select **Jenkins**.

Step 4 Configure the GitLab account password and click **Add** to save the configuration.

Step 5 Choose **Manage Jenkins > Manage Credentials** to view the configured credentials.

The unique ID is used in [Configuring a Pipeline Script](#).

----End

Creating a Pipeline Task

Step 1 Enter **http://*{IP address of the Linux VM where Jenkins is installed}*:8080** in the address box of the browser to log in to Jenkins.

Step 2 Click **New Item**.

Step 3 Enter the task name, for example, **test-upgrade**, select **Pipeline**, and click **OK**.

----End

Configuring a Build Trigger

Step 1 Configure the Jenkins build trigger.

1. Select **Build when a change is pushed to GitLab**, save the GitLab webhook URL (required when configuring GitLab webhook), and click **Advanced** in the lower right corner.
2. Select **Filter branches by regex** and configure the build task to be triggered after the specified branch is changed. In the example, the branch name is **main**. Click **Generate** to generate a secret token and save it. The token will be used for configuring GitLab webhook.

Step 2 Configure GitLab webhook.

1. Log in to GitLab and go to the code repository. In the example, the repository name is **test**. Select **Webhooks** in **settings**, and set **URL** and **Secret token** to the GitLab webhook URL and secret token obtained in **Step 1**.
2. Deselect **Enable SSL verification** for **SSL verification** and click **Add webhook**.

----End

Configuring a Pipeline Script

A pipeline script is a build command that runs during build. For details about script parameters, see [Table 6-3](#).

Table 6-3 Table 1 Pipeline script parameters

Parameter	Mandatory	Type	Description
git_url	Yes	String	Address of the GitLab code repository.
credentials_id	Yes	String	GitLab credential ID configured using the account password. For details, see Creating a GitLab Credential .
branch_name	Yes	String	Name of the GitLab code repository branch .
maven	Yes	String	Path of the executable file for Maven installation, for example, /root/app/maven/apache-maven-3.8.6/bin/mvn .
upgrade_script	Yes	String	Path for storing the upgrade.sh script on the VM where Jenkins is deployed, for example, /root/jar/upgrade.sh . For details, see upgrade.sh Description .

Step 1 After the build trigger is configured, select **Pipeline script** from the drop-down list on the **Pipeline** tab.

Step 2 Configure the pipeline script. In the example, the JAR package build scenario is used. The script is as follows:

Replace the parameters in the script with the actual parameters in your environment.

```
node {
  //Code repository address, for example, http://10.95.156.58:8090/zmg/test.git.
  def git_url = '{Code repository address}'
  //GitLab credential ID.
  def credentials_id = '{GitLab credential ID}'
  //Name of the Git code repository branch, for example, main.
  def branch_name = '{Git code repository branch name}'
  //Path of the executable file for Maven installation, for example, /root/app/maven/apache-
  maven-3.8.6/bin/mvn.
  def maven = '{Path of the executable file for Maven installation}'
  //Path for storing the upgrade.sh script, for example, /root/jar/upgrade.sh.
  def upgrade_shell = '{Path for storing the upgrade.sh script}'

  stage('Clone sources') {
    git branch: branch_name, credentialsId: credentials_id, url: git_url
  }
  stage('Build') {
    //Build a JAR package.
    sh "$maven clean package -Dmaven.test.failure.ignore=true -Dmaven.wagon.http.ssl.insecure=true -
    Dmaven.wagon.http.ssl.allowall=true"
  }
  stage('upgrade') {
    //Execute the script and use the JAR package uploaded to OBS to upgrade the ServiceStage
    component. The timeout period is 5 minutes.
    sh "timeout 300s $upgrade_shell"
  }
}
```

NOTE

- During pipeline script running, **upgrade.sh** is invoked. For details about the script, see [upgrade.sh Description](#) .
- Set **upgrade.sh** as an executable file.

----End

6.3.3 upgrade.sh Description

Script Content

Replace the parameters in the script with the actual parameters in your environment.

```
#!/bin/bash
#Project ID
project_id='{Project ID}'
#Application ID
application_id='{Application ID}'
#Component ID
component_id='{Component ID}'
#Batch information
rolling_release_batches=1
#Deployment type
deploy_type="package"

### Description:
### 1. Search for a string, as shown in key in the following code. If no string is found, defaultValue is
returned.
### 2. Search for the nearest colon (:). The content following the colon is the value.
### 3. If there are multiple keys with the same name, only the first value is printed.
###
### 4. params: json, key, defaultValue
function getJsonValuesByAwk() {
  awk -v json="$1" -v key="$2" -v defaultValue="$3" 'BEGIN{
    foundKeyCount = 0
```

```

pos = match(json, "\"\"key\"\"[ \\t]*?:[ \\t]*");
if (pos == 0) {if (foundKeyCount == 0) {print defaultValue;} exit 0;}

++foundKeyCount;
start = 0; stop = 0; layer = 0;
for (i = pos + length(key) + 1; i <= length(json); ++i) {
  lastChar = substr(json, i - 1, 1)
  currChar = substr(json, i, 1)

  if (start <= 0) {
    if (lastChar == ":") {
      start = currChar == " " ? i + 1;
      if (currChar == "{" || currChar == "[") {
        layer = 1;
      }
    }
  } else {
    if (currChar == "{" || currChar == "[") {
      ++layer;
    }
    if (currChar == "}" || currChar == "]") {
      --layer;
    }
    if ((currChar == "," || currChar == ";" || currChar == "]") && layer <= 0) {
      stop = currChar == "," ? i + 1 + layer;
      break;
    }
  }
}

if (start <= 0 || stop <= 0 || start > length(json) || stop > length(json) || start >= stop) {
  if (foundKeyCount == 0) {print defaultValue;} exit 0;
} else {
  print substr(json, start, stop-start);
}
}'
}

#Query component information.
function GetComponentInfo() {
  #Query component information.
  component_details="hcloud ServiceStage ShowComponentInfo/v3 --project_id="$project_id" --
application_id="$application_id" --component_id="$component_id"

  #Print component information.
  echo "$component_details"

  #Obtain the component name.
  test_name=`getJsonValuesByAwk "$component_details" "name" "defaultValue"
lenj=${#test_name}
component_name=${test_name:1:lenj-2}
echo "name : $component_name"

  data_time=$(date +%Y.%m.%d.%H%M)
  seconds=$(date +%S)
  component_version="${data_time}${seconds:1:1}"
  echo "version: $component_version"
}

#Image deployment scenario
function swr_image_upgrade() {

  #Image generated after project packaging: Image name:Version name
  machine_image_name='java-test:v1'
  #Path of the SWR image repository to which the image is uploaded
  swr_image_url='{Image repository address}/{Organization name}/{Image name}:{Version}'
  #AK, which is used to log in to the SWR image repository.
  AK='BMCKUPO9HZMI6BRDJGBD'

```



```
#SWR login key, which is used to log in to the SWR image repository
SK=${SWR login key}'
#SWR image repository address
swr_url='{SWR image repository address}'
#Region
region="{Region}"

echo "upload image to swr"
docker tag "$machine_image_name" "$swr_image_url"

login_secret=`printf "$AK" | openssl dgst -binary -sha256 -hmac "$SK" | od -An -vtx1 | sed 's/[ \n]//g' |
sed 'N;s/\n//`

login_result=`docker login -u "$region"@"$AK" -p "$login_secret" "$swr_url"`
#Print the result of logging in to the SWR image repository.
echo "$login_result"
push_result=`docker push "$swr_image_url"`
#Print the image push result.
#echo "$push_result"
logout_result=`docker logout "$swr_url"`
#Print the result of logging out of the SWR image repository.
echo "$logout_result"
#Clear all historical records. They may contain SWR login key information.
#history -c

echo "upgrade component"

action_result=`hcloud ServiceStage ModifyComponent/v3 --project_id="$project_id" --
application_id="$application_id" --component_id="$component_id" --version="$component_version" --
runtime_stack.name="Docker" --runtime_stack.type="Docker" --source.kind="image" --
source.storage="swr" --source.url="$swr_image_url" --name="$component_name" --
deploy_strategy.rolling_release.batches=$rolling_release_batches --deploy_strategy.type="RollingRelease" `
}

#JAR package deployment scenario
function obs_jar_upgrade() {

#Absolute path of the executable file for installing obsutil
obsutil='/root/tools/obsutil/obsutil_linux_amd64_5.4.6/obsutil'
#OBS bucket name
bucket='obs://{OBS bucket name}'
echo "upload jar to obs"
#Upload the JAR package generated in the project to OBS.
obs_result=`$obsutil cp ./target/*.jar "$bucket"`
#Print the upload result.
echo "$obs_result"
#Link of the JAR package uploaded to OBS
obs_jar_url='obs://{OBS bucket name}/{Jar package name}'

echo "upgrade component"

action_result=`hcloud ServiceStage ModifyComponent/v3 --project_id="$project_id" --
application_id="$application_id" --component_id="$component_id" --version="$component_version" --
runtime_stack.name="OpenJDK8" --runtime_stack.type="Java" --source.kind="package" --
source.storage="obs" --source.url="$obs_jar_url" --name="$component_name" --
deploy_strategy.rolling_release.batches=$rolling_release_batches --deploy_strategy.type="RollingRelease" `
}

#Query the job status every 15 seconds until the job is complete.
function waitDeployFinish() {
sleep 10s
id="$1"
leni=${#id}
id=${id:1:leni-2}
echo "job_id= $id"
job_status=""
while [[ "$job_status" != "SUCCEEDED" ]]; do
```

```

job_status_result=`hcloud ServiceStage ShowJobDetail/v2 --project_id="$project_id" --job_id="$id"`
job_status=`getJsonValuesByAwk "$job_status_result" "EXECUTION_STATUS" "defaultValue"`
lenj=${#job_status}
job_status=${job_status:1:lenj-2}
echo "$job_status"
if [[ "$job_status" != "RUNNING" && "$job_status" != "SUCCEEDED" ]]; then
    echo 'Deployment failed.'
    echo "$job_status_result"
    return
fi
sleep 15s
done
echo 'Deployment succeeded.'
}

function upgradeTask() {
    if [[ "$deploy_type" == "package" ]]; then
        obs_jar_upgrade
    elif [[ "$deploy_type" == "image" ]]; then
        swr_image_upgrade
    else
        return
    fi
    #Print the component upgrade result.
    echo "$action_result"
    #Obtain the job_id in the result.
    job_id=`getJsonValuesByAwk "$action_result" "job_id" "defaultValue"`
    echo "$job_id"
    #Wait until the upgrade is complete.
    waitDeployFinish "$job_id"
}

function main() {
    getComponentInfo
    upgradeTask
}

main

```

Script Parameters

Parameter	Mandatory	Type	Description
region	Yes	String	Region name. For details, see Obtaining Values .
project_id	Yes	String	Project ID. For details, see Obtaining Values .
application_id	Yes	String	Application ID. For details, see Obtaining Values .
component_id	Yes	String	Component ID. For details, see Obtaining Values .
rolling_release_batches	Yes	int	Deployment batches.

Parameter	Mandatory	Type	Description
deploy_type	Yes	String	Deployment type. <ul style="list-style-type: none"> • package • image
obsutil	No	String	Absolute path for uploading JAR packages to OBS. This parameter is mandatory when software packages, such as JAR packages, are used for deployment. For example, /root/tools/obsutil/obsutil_linux_amd64_5.4.6/obsutil .
bucket	No	String	Path of the OBS bucket to which the package is uploaded. This parameter is mandatory when software packages are used for deployment. The format is obs://{Bucket name} . For example, obs://obs-mzc .
obs_jar_url	No	String	Link after the software package is uploaded to OBS. This parameter is mandatory when software packages are used for deployment. The format is obs://{Bucket name}/{Software package name} . For example: obs://obs-mzc/spring-demo-0.0.1-SNAPSHOT.jar
machine_image_name	No	String	Image generated after Jenkins packaging and build. This parameter is mandatory when images are used for deployment. The format is <i>{Image name}: {Version}</i> . For example, java-test:v1 .
swr_image_url	No	String	Path of the image package uploaded to the SWR image repository. This parameter is mandatory when images are used for deployment. The format is <i>{Image repository address}/{Organization name}/{Image package name}:{Version}</i> . The format of SWR image repository address is swr.{Project name of the region}.myhuaweicloud.com .
AK	No	String	AK, which is used to log in to the SWR image repository. This parameter is mandatory when images are used for deployment. For details, see Access Keys .
SK	No	String	SK, which is used together with AK to log in to the SWR image repository. This parameter is mandatory when images are used for deployment. For details, see Access Keys .

Parameter	Mandatory	Type	Description
login_secret	No	String	Key for logging in to the SWR image repository. This parameter is mandatory when images are used for deployment. Run the following command. The returned result is the login key. <pre>printf "{AK}" openssl dgst -binary -sha256 -hmac "{SK}" od -An -vtx1 sed 's/[\n]//g' sed 'N;s/\n/'</pre> Replace {AK} and {SK} with the obtained AK and SK.
swr_url	No	String	SWR image repository address. This parameter is mandatory when images are used for deployment. The format is swr.{Project name of the region}.myhuaweicloud.com .

Obtaining Values

- Obtain **region** and **project_id**.
 - a. Log in to ServiceStage.
 - b. Move the cursor to the username in the upper right corner and select **My Credentials** from the drop-down list.
 - c. View the project and project ID of the region, that is, the values of **region** and **project_id**.
- Obtain **application_id** and **component_id**.
 - a. Log in to ServiceStage.
 - b. Choose **Component Management**.
 - c. Click the corresponding component.
 - d. In the **Configurations** area of the **Overview** page, click **Component Configuration**.
View **CAS_APP_ID** and **CAS_APPLICATION_ID**, that is, the values of **application_id** and **component_id**.

6.4 Build Verification

6.4.1 Manual Build

- Step 1** Enter **http://{IP address of the Linux VM where Jenkins is installed}:8080** in the address box of the browser to log in to Jenkins.
- Step 2** Click **My View**.
- Step 3** Click the corresponding build task to go to the details page.
- Step 4** Click **Build Now** to generate the build task.

The corresponding build task information is displayed in the **Build History** and **Stage View** areas. Move the cursor to a step to display the task status and log button. Click **log** to view logs.

Step 5 Log in to ServiceStage.

Step 6 Choose **Component Management**.

Step 7 In the **Component List** area, click the target component. The component overview page is displayed.

On the **Overview** page, check whether the component version and component package code source have been updated.

Step 8 Click **Deployment Record** to view the corresponding deployment record.

----End

6.4.2 Jenkins Build Triggered by GitLab

GitLab triggers Jenkins build in either of the following methods:

- Method 1: Use the configured webhook to push events and trigger Jenkins build task.
- Method 2: Modify the file of the specified branch in the build configuration to push events and trigger Jenkins build task.

This section uses method 1 as an example.

Procedure

Step 1 Log in to GitLab and go to the code repository.

Step 2 Click **Settings**, select **Webhooks**, and select **Push events** from the **Test** drop-down list.

Step 3 Enter **http://*{IP address of the Linux VM where Jenkins is installed}*:8080** in the address box of the browser to log in to Jenkins.

In the build execution status on the left, you can view the build tasks that have been triggered.

Step 4 Click the build task ID and choose **Console Output** to view the build output logs.

Step 5 Log in to ServiceStage.

Step 6 Choose **Component Management**.

Step 7 In the **Component List** area, click the target component. The component overview page is displayed.

On the **Overview** page, check whether the component version and component package code source have been updated.

Step 8 Click **Deployment Record** to view the corresponding deployment record.

----End