

Flexus L Instance

Best Practices

Issue 01
Date 2025-02-14



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. 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 Best Practices for FlexusL.....	1
2 Setting Up a Website.....	3
2.1 Managing Servers Using the BT Panel.....	3
2.2 Building a WordPress Website.....	13
2.3 Using Matomo to Build a Website Traffic Statistics System.....	31
2.4 Using Odoo to Build an ERP System.....	40
2.5 Using Moodle to Build an Online Learning System.....	53
2.6 Using Joomla to Build a Content Management System.....	61
2.7 Using Ghost to Build a Personal Blog.....	71
2.8 Using EspoCRM to Build a Content Management System.....	81
3 Setting Up the Development Environment.....	90
3.1 Using Portainer to Deploy a MySQL Container.....	90
3.2 Using Node.js to Run Node.js Programs.....	99
4 Setting Up an Application.....	105
4.1 Project Management Scenarios.....	105
4.1.1 Using GitLab to Manage Teams and Projects.....	105
4.1.2 Using Redmine to Create a Project.....	119
4.2 Cloud Disk Scenarios.....	127
4.2.1 Using Nextcloud to Set Up an Enterprise Web Disk System.....	128
4.2.2 Using Kodbox to Quickly Set Up a Cloud Disk.....	136
4.3 E-commerce.....	141
4.3.1 Using Windows Server to Set Up a Cross-Border E-Commerce Store.....	141
4.3.2 Using PrestaShop to Build an E-Commerce Website.....	149
4.4 Audio and Video Scenarios.....	161
4.4.1 Pushing Local PC Desktop Streams to SRS Using OBS.....	161
4.5 Website Data Analysis.....	172
4.5.1 Using Superset to Obtain Data from MySQL for Analysis.....	172
5 Server Migration.....	184
5.1 Using Images to Migrate FlexusL Instances to ECSs	184
5.2 Using SMS to Migrate Servers to FlexusL Instances.....	190

1 Best Practices for FlexusL

After purchasing a FlexusL instance, you can build environments on it. This document describes how to set up a website and development environment based on FlexusL instances.

Table 1-1 Best practices

Item	Helpful Link
Setting Up a Website	<ul style="list-style-type: none">• Managing Servers Using the BT Panel• Building a WordPress Website• Using Matomo to Build a Website Traffic Statistics System• Using Odoo to Build an ERP System• Using Moodle to Build an Online Learning System• Using Joomla to Build a Content Management System• Using Ghost to Build a Personal Blog• Using EspoCRM to Build a Content Management System
Setting Up the Development Environment	<ul style="list-style-type: none">• Using Portainer to Deploy a MySQL Container• Using Node.js to Run Node.js Programs

Item	Helpful Link
<p>Setting Up an Application</p>	<p>Project management scenarios</p> <ul style="list-style-type: none"> ● Using GitLab to Manage Teams and Projects ● Using Redmine to Create a Project <p>Cloud disk scenarios</p> <ul style="list-style-type: none"> ● Using Nextcloud to Set Up an Enterprise Web Disk System ● Using Kodbox to Quickly Set Up a Cloud Disk <p>E-commerce</p> <ul style="list-style-type: none"> ● Using Windows Server to Set Up a Cross-Border E-Commerce Store ● Using PrestaShop to Build an E-Commerce Website <p>Audio and video scenarios</p> <p>Pushing Local PC Desktop Streams to SRS Using OBS</p> <p>Website data analysis</p> <p>Using Superset to Obtain Data from MySQL for Analysis</p>
<p>Server Migration</p>	<ul style="list-style-type: none"> ● Using Images to Migrate FlexusL Instances to ECSs ● Using SMS to Migrate Servers to FlexusL Instances

2 Setting Up a Website

2.1 Managing Servers Using the BT Panel

Application Scenario

The BT panel is a visualized server management software that supports more than 100 server management functions, such as one-click LAMP, LNMP, monitoring, website, FTP, database, and Java. Supported By FlexusL, the BT panel application image uses Ubuntu 22.04 and provides a web client for you to manage servers, such as website or file management, graphical monitoring, and task planning. You can use this application image to manage servers.

Resource Planning and Costs

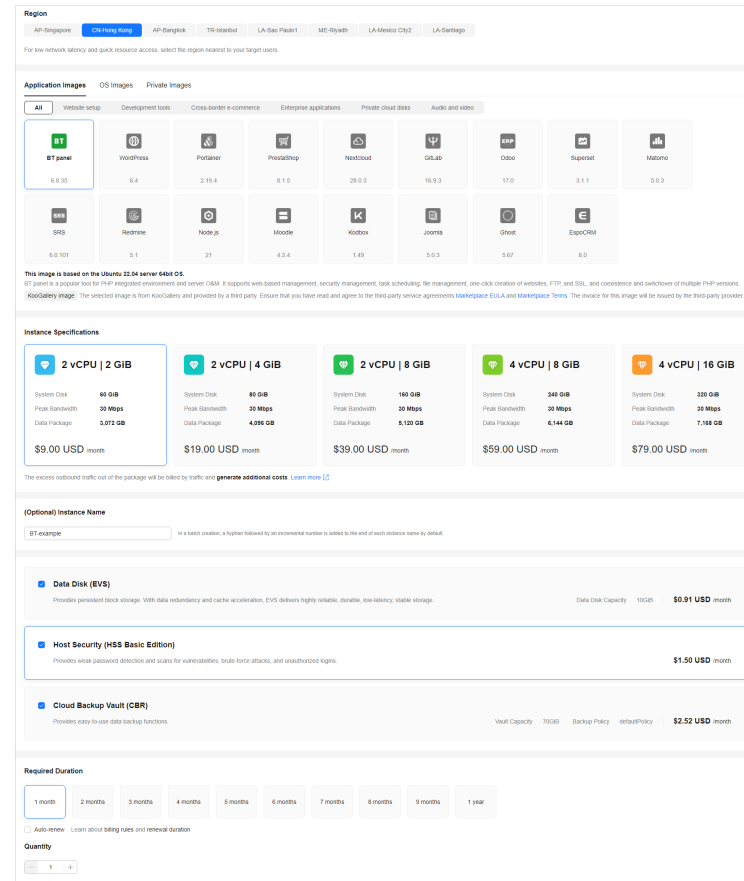
Resource	Configuration	Description
Cloud server	<ul style="list-style-type: none">vCPUs: 2Memory: 2 GiB	A BT panel application image requires at least 2 vCPUs and 2 GiB of memory. Select appropriate instance specifications accordingly.
Image	BT panel	Select the BT panel application image.
Security group	<p>Inbound rule:</p> <ul style="list-style-type: none">Protocol/ Application: TCPPort: 80, 443, 8888, 3306, or 9090Source: 0.0.0.0/0	<ul style="list-style-type: none">80: Allows HTTP traffic to FlexusL instances.443: Allows HTTPS traffic to FlexusL instances.8888: Allows access to the BT panel.3306: Allows access to MySQL databases.9090: Allows access to the phpMyAdmin database management tool

Process

Procedure	Description
Step 1: Purchase a FlexusL Instance	Purchase a FlexusL instance and select the BT panel application image.
Step 2: Configure a Security Group	Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.
Step 3: Reset the Password and Log In to the FlexusL Instance	A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance before logging in to it.
Step 4: Initialize the BT Panel	Log in to the BT dashboard and install the basic software bundle.
Step 5: Deploy the BT Panel	On the dashboard, perform the following operations: <ul style="list-style-type: none">• Configure domain names.• Install an SSL certificate for your website.• Manage software.• Manage files.• Manage logs.

Step 1: Purchase a FlexusL Instance

1. Log in to the FlexusL [console](#) and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



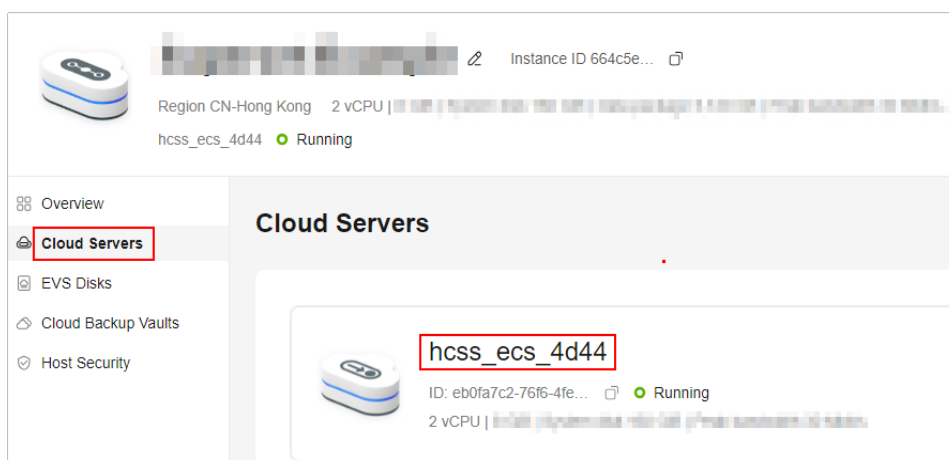
Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Application Image	BT panel	Select the BT panel application image.
Instance Specifications	2 vCPUs 2 GiB of memory and 60 GiB system disk	Select instance specifications as needed.
Instance Name	BT-Example	Customize an instance name that is easy to identify, for example, BT-Example.

Parameter	Example	Description
(Optional) Associated Services	<ul style="list-style-type: none"> Data disk: 10 GiB Host security Cloud backup vault: 70 GiB 	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure a Security Group

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.

The following figure only displays common rules. You can add more rules as needed.

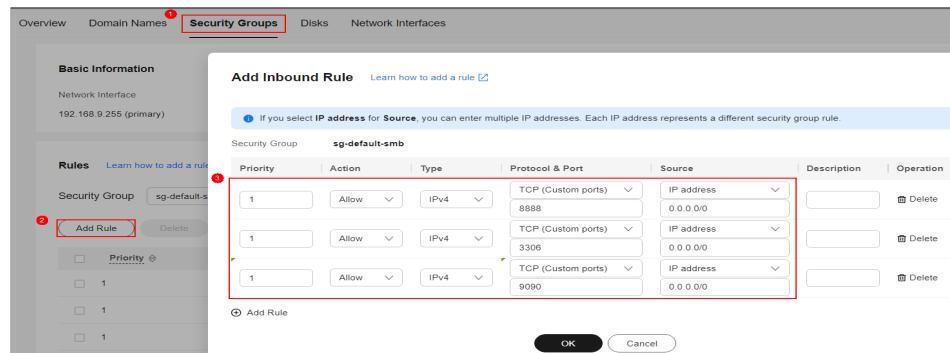


Table 2-1 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 3306	0.0.0.0/0	Allows access to MySQL databases.
1	Allow	IPv4	TCP: 9090	0.0.0.0/0	Allows access to the phpMyAdmin database management tool.
1	Allow	IPv4	TCP: 8888	0.0.0.0/0	Allows access to the BT panel dashboard.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS traffic to FlexusL instances.
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Allows HTTP traffic to FlexusL instances.

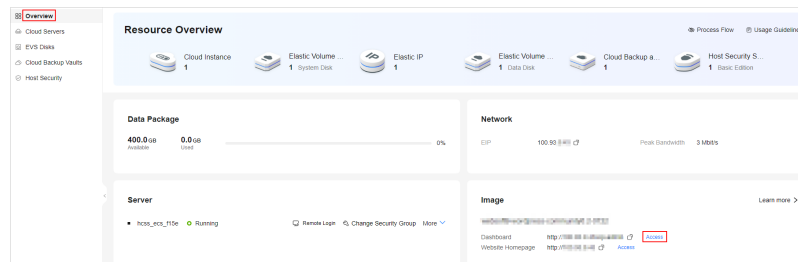
Step 3: Reset the Password and Log In to the FlexusL Instance

This section describes how to log in to a FlexusL instance. A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance before logging in to it.

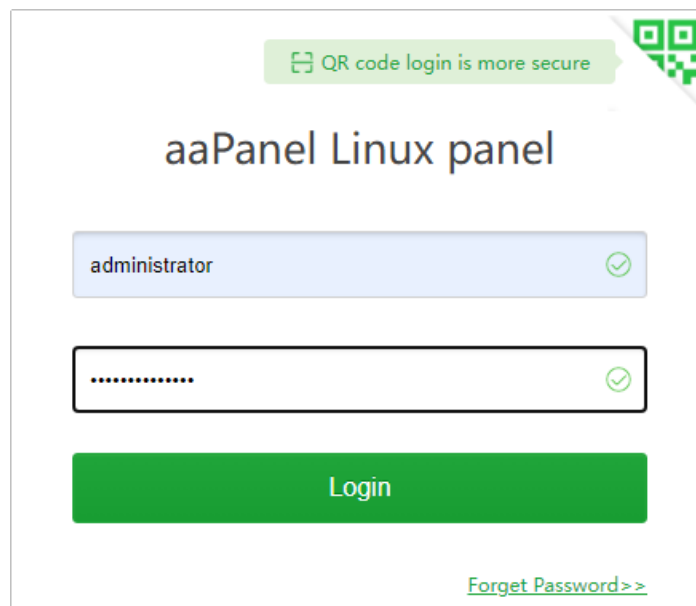
1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard and check whether the application has been up and running. If yes, go to the next step.

NOTICE

Wait for several minutes until the image with the pre-installed application is up and running. Then, you can perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the initial password may become invalid and you cannot log in to the application dashboard.

Figure 2-1 Entry to the application dashboard

After the application is started, the initialization wizard page of the dashboard is displayed.

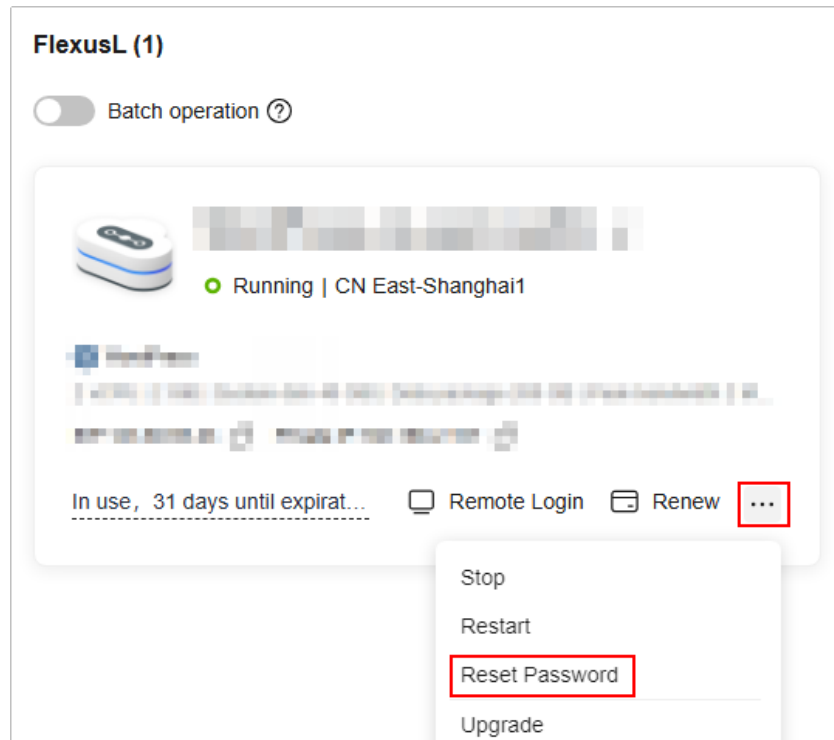
**NOTE**

If the dashboard is not properly displayed, check the following causes:

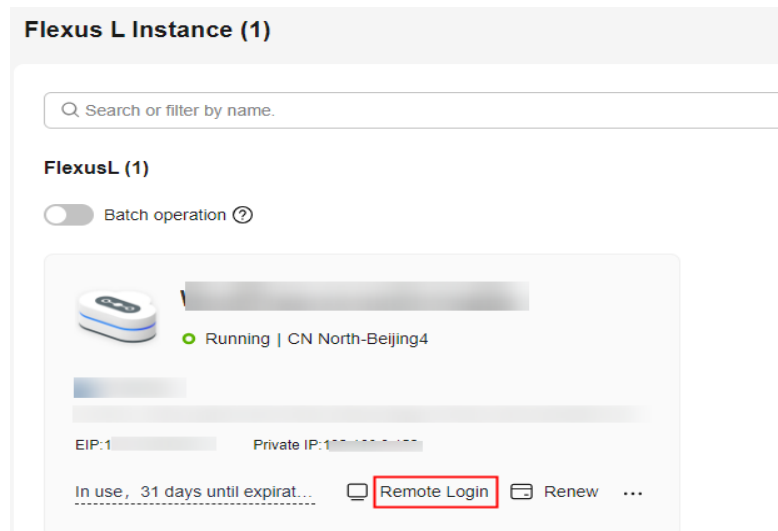
- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure a Security Group](#).
 - The dashboard is being started. Try again later.
2. Locate the resource card and choose **...** > **Reset Password** to reset the password.

A FlexusL instance does not have an initial password. Set a password for the FlexusL instance before logging in to it. For details, see [Resetting the Password for a FlexusL Instance](#).

Figure 2-2 Resetting a password



3. Locate the target instance and click **Remote Login** and enter the username and password as prompted to log in to the FlexusL instance. The username is **root**, and the password is the one set in 2.



Step 4: Initialize the BT Panel

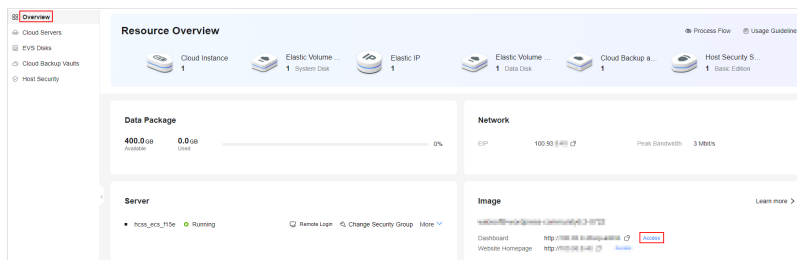
Application images use code-based Ubuntu. They provide graphical user interfaces to make your operations easier. You need to initialize the application dashboard upon the first login. Then you can directly log in to the dashboard from the FlexusL console afterwards.

1. Obtain the administrator username and password for logging in to the BT panel.

Log in to the server and run `sudo cat /credentials/password.txt` to obtain the username and password for logging in to the BT panel.

```
root@smb-ecs-3a7a:~# sudo cat /credentials/password.txt
===== credentials for bt =====
bt_user: administrator
bt_password: iaXqt
root@smb-ecs-3a7a:~# _
```

2. On the **Overview** page, click **Access** in the **Dashboard** field in the **Image** area.

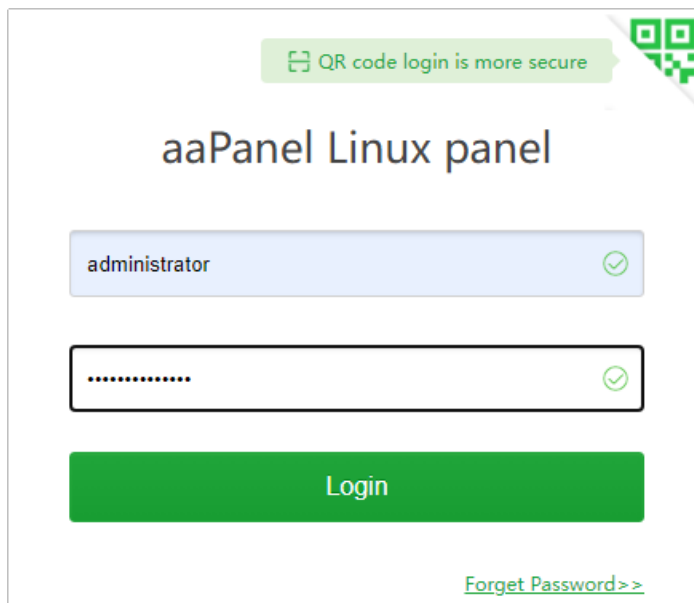


NOTE

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure a Security Group](#).
- The dashboard is being started. Try again later.

3. Enter the username and password obtained in **1** and click **Login**.



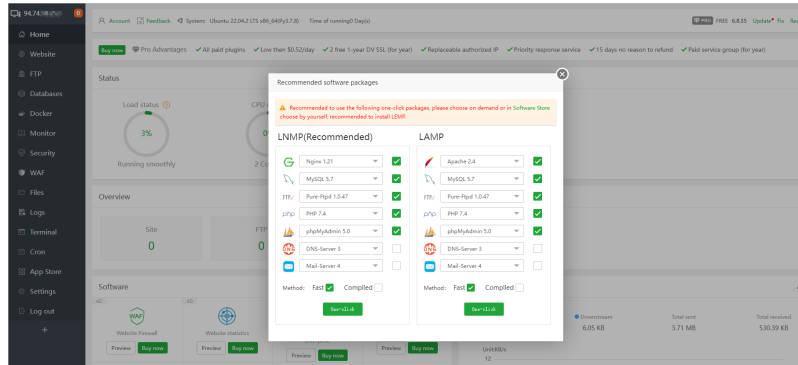
NOTE

If a message is displayed indicating that the username or password you entered is invalid when you attempt to log in to the application dashboard, refer to [Why Can't I Access the Dashboard of the Application Pre-installed in the Application Image After Entering the Initial Username and Password?](#)

4. Install the basic software bundle.

You can select recommended software packages and click **One-click** to install them when you log in to the dashboard for the first time.

You can also close the popup and select other software from **App Store** and install them afterwards.



After the initialization of the BT panel application is complete, you can deploy applications on the dashboard.

Step 5: Deploy the BT Panel

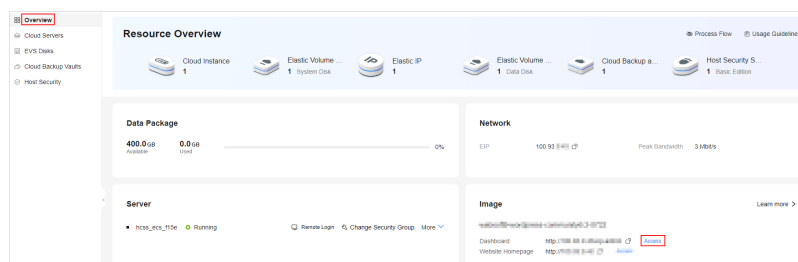
Configuring Domain Names

If you want to use a domain name to access a website, add and resolve the domain name for the website.

1. If the domain name is not registered with Huawei Cloud or not hosted on Huawei Cloud DNS, the domain name cannot be resolved. Use either of the following methods to resolve the issue:
 - Contact the DNS service provider to add an A record that maps the domain name to the EIP of the FlexusL instance.
 - Use Huawei Cloud DNS servers to resolve the domain name. For details, see [Migrating to Huawei Cloud DNS for Domain Name Resolution](#).
2. Configure the domain name on the application dashboard.

If you had added a domain name to a cloud server, or removed a domain name from a cloud server and then add a new one, you need to configure the domain name on the application management page so that the domain name can be used to access the website.

- a. On the **Overview** page, click **Access** in the **Dashboard** field in the **Image** area.

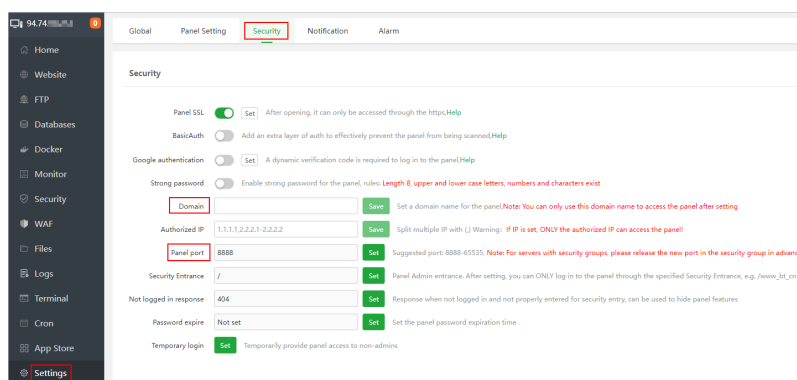


NOTE

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure a Security Group](#).
 - The dashboard is being started. Try again later.
- b. Choose **Settings > Security**, enter a domain name for **Domain**, for example, **www.wpwebsite.com**, and click **Save**.

The BT panel uses port 8888 by default. If you want to use the domain name to access the website directly, you need to change the port number to the default HTTP or HTTPS port (80 or 443). If you do not change the port number, you need to access the website through **http://Domain-name:8888** or **https://Domain-name:8888**.



Installing an SSL Certificate for Your Website

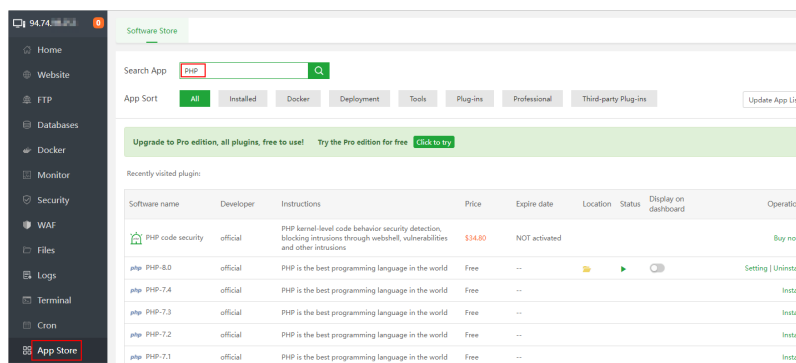
BT panel uses HTTPS by default, and you do not need to install an SSL certificate.

Managing Software

In the software store, you can install, uninstall, and manage software.

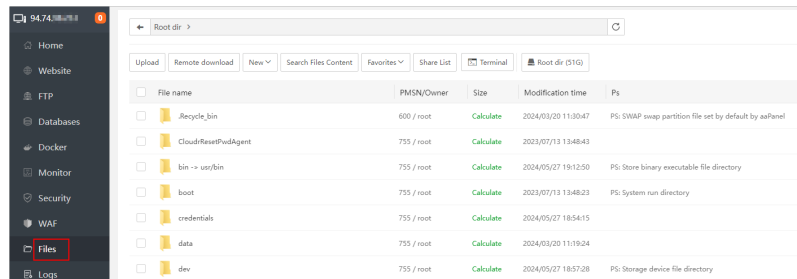
You can search for the software by name or category. A PHP extension plugin is required to enhance PHP language functions. The following shows how to install a PHP extension:

1. Choose **App Store** in the left navigation pane and search for PHP.
2. Select the PHP version, click **Install** or **Buy now** in the **Operation** column of the target software and complete the installation.



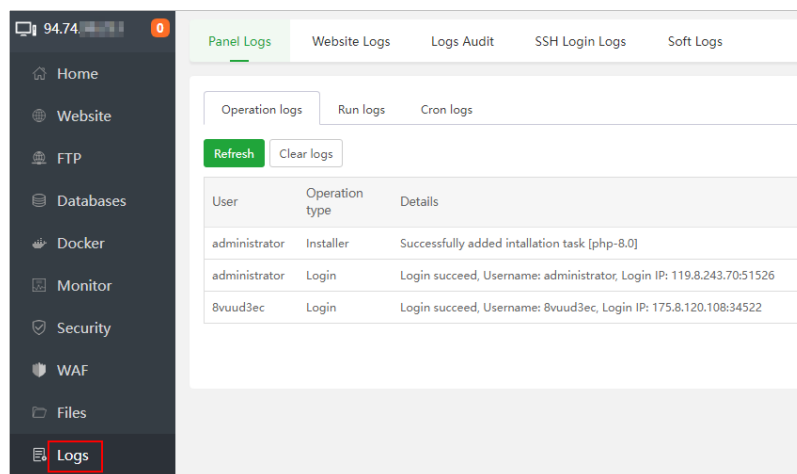
Managing Files

In the **Files** menu, you can perform a range of operations on files, including copying, pasting, cutting, deleting, renaming, compressing, refreshing, or creating a file, and creating a directory for a file.



Managing Logs

In the **Logs** menu, logs are classified by log type. You can click the tabs to view different types of logs and clear logs.



2.2 Building a WordPress Website

Application Scenario

WordPress is an enterprise-level open-source content management system. It is usually used for enterprise website setup, cross-border e-commerce, and personal blog building. Supported By FlexusL, the WordPress application image uses Ubuntu 22.04 and is deployed using Docker. The Nginx, MySQL, phpMyAdmin, and Docker have been preconfigured in the image. You can use this application image to quickly set up a website.

Resource Planning and Costs

This practice uses the following resource planning as an example. You can adjust it as required.

Resource	Configuration	Description
Cloud server	<ul style="list-style-type: none">vCPUs: 2Memory: 2 GiB	Select appropriate instance specifications based on your service requirements.
Image	WordPress	Select the WordPress application image.
Security group	Inbound rule: <ul style="list-style-type: none">Protocol: TCPPorts: 443, 80, 9000, 9001, and 3306Source: 0.0.0.0/0	<ul style="list-style-type: none">443: Allows HTTPS traffic to a website.3306: Allows access to MySQL databases.80: Specifies the internal forwarding port of application images.9000: Allows external access to the application O&M page.9001: Allows external access to the application dashboard.
Domain name	wpwebsite.com	<ul style="list-style-type: none">If the website is only used for personal development or testing, there is no need to add a domain name.If the website is open to the public, add and resolve a domain name for the cloud server.

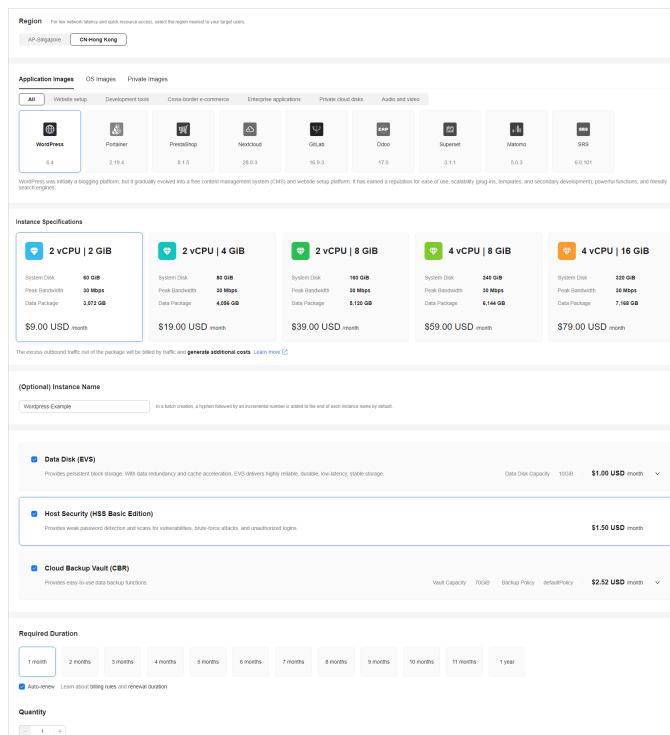
Process

Procedure	Description
Step 1: Purchase a FlexusL Instance	Purchase a FlexusL instance and select the WordPress application image.
Step 2: Configure a Security Group	Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.
Step 3: Reset the Password and Log In to the FlexusL Instance	A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance before logging in to it.
Step 4: Initialize WordPress	Log in to the dashboard, set the username and password, and install WordPress. The image application dashboard needs to be initialized only when you log in for the first time.

Procedure	Description
Step 5: Operate Websites	<p>On the dashboard, perform the following operations:</p> <ul style="list-style-type: none"> • Configure domain names. • Install an SSL certificate for your website. • Manage appearance. • Manage plug-ins. • Configure SMTP. • Reset a password.

Step 1: Purchase a FlexusL Instance

1. Log in to the FlexusL **console** and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Applicati on Image	WordPress	Select the WordPress application image.

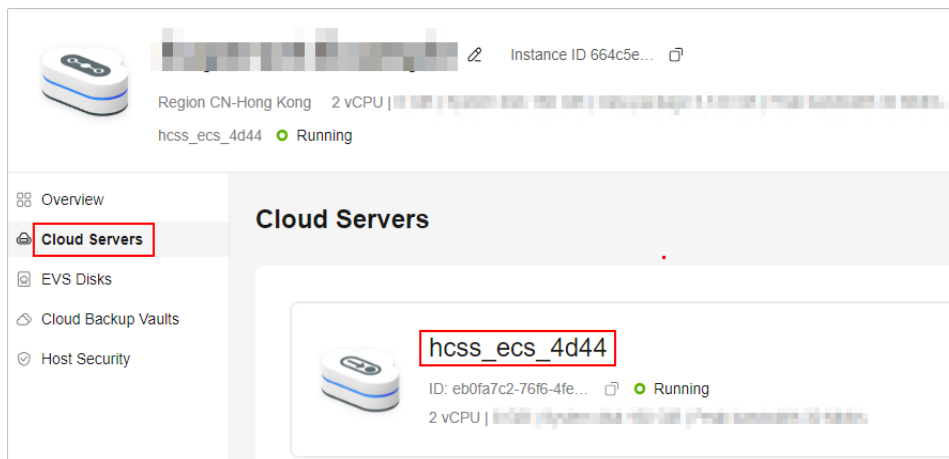
Parameter	Example	Description
Instance Specifications	2 vCPUs 2 GiB memory and 60 GiB system disk	Select instance specifications as needed.
Instance Name	Wordpress-Example	Customize an instance name that is easy to identify, for example, Wordpress-Example.
(Optional) Associated Services	<ul style="list-style-type: none">• Data disk: 10 GiB• Host security• Cloud backup vault: 70 GiB	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure a Security Group

Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.

The following figure only displays common rules. You can add more rules as needed.

Table 2-2 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 3306	0.0.0.0/0	Allows access to MySQL databases.
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of application images
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS access to the application dashboard.
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M page.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

Step 3: Reset the Password and Log In to the FlexusL Instance

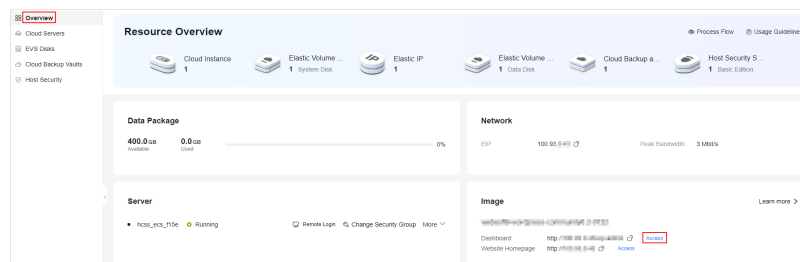
This section describes how to log in to a FlexusL instance. A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance before logging in to it.

1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard and check whether the application has been up and running. If yes, go to the next step.

NOTICE

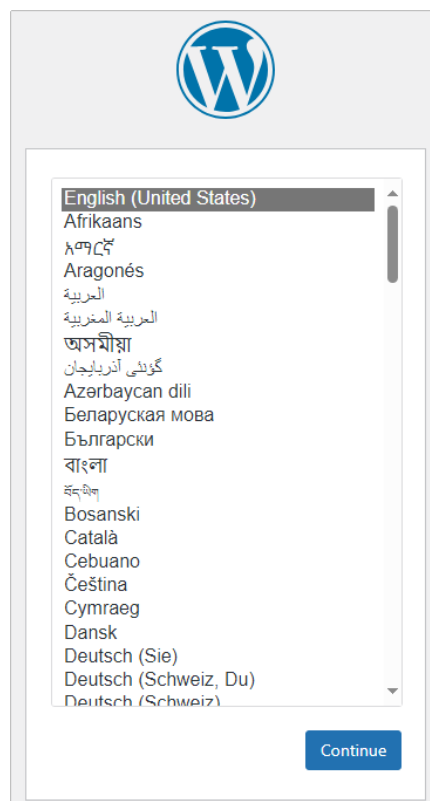
Wait for several minutes until the image with the pre-installed application is up and running. Then, you can perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the initial password may become invalid and you cannot log in to the application dashboard.

Figure 2-3 Entry to the application dashboard



After the application is started, the initialization wizard page of the dashboard is displayed, as shown in **Figure 2-4**.

Figure 2-4 Initialization wizard page of the WordPress dashboard



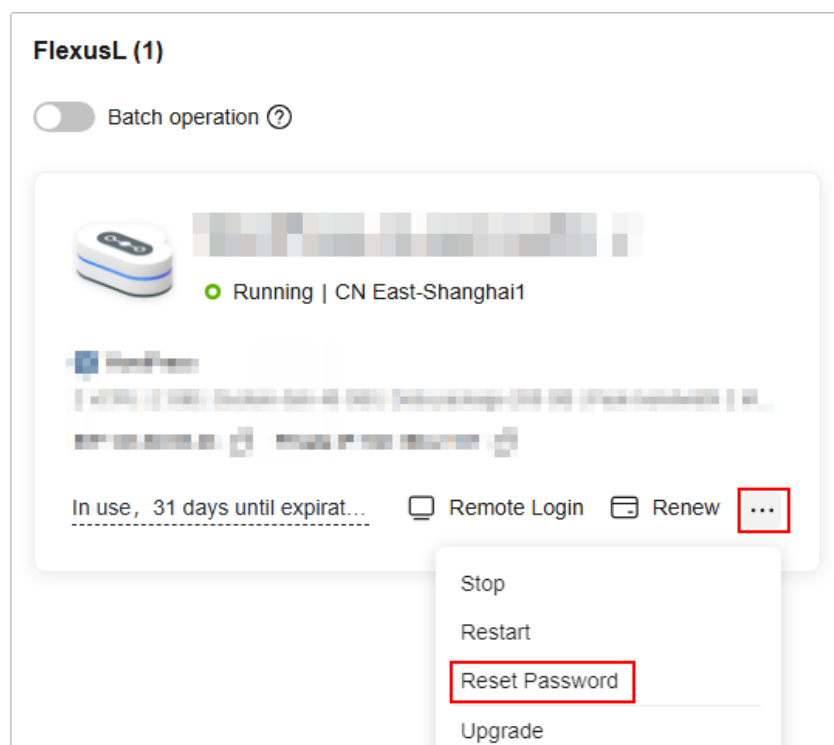
NOTE

If the dashboard is not properly displayed, check the following causes:

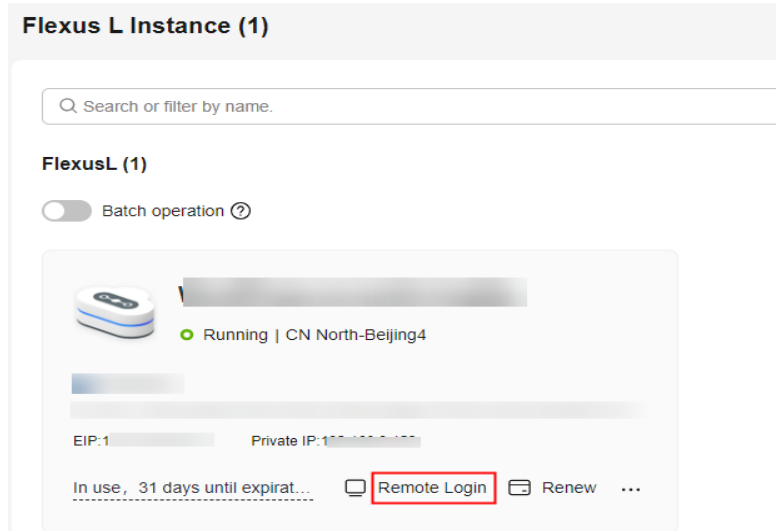
- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure a Security Group](#).
 - The dashboard is being started. Try again later.
2. Locate the resource card and choose **...** > **Reset Password** to reset the password.

A FlexusL instance does not have an initial password. Set a password for the FlexusL instance before logging in to it. For details, see [Resetting the Password for a FlexusL Instance](#).

Figure 2-5 Resetting a password



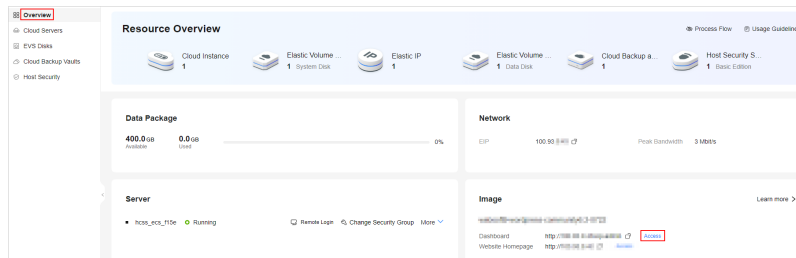
3. Locate the target instance and click **Remote Login** and enter the username and password as prompted to log in to the FlexusL instance. The username is **root**, and the password is the one set in [2](#).



Step 4: Initialize WordPress

Application images use code-based Ubuntu. They provide graphical user interfaces to make your operations easier. You need to initialize the application dashboard upon the first login. Then you can directly log in to the dashboard from the FlexusL console afterwards.

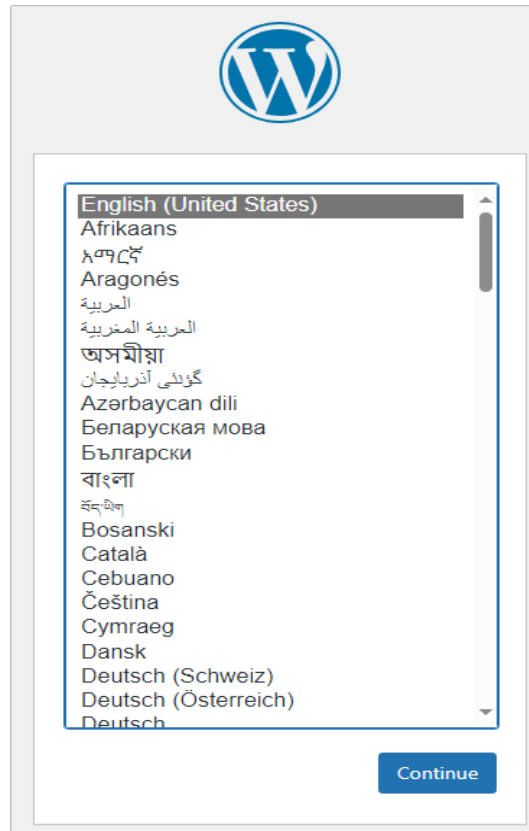
1. On the **Overview** page, click **Access** in the **Dashboard** field in the **Image** area.



NOTE

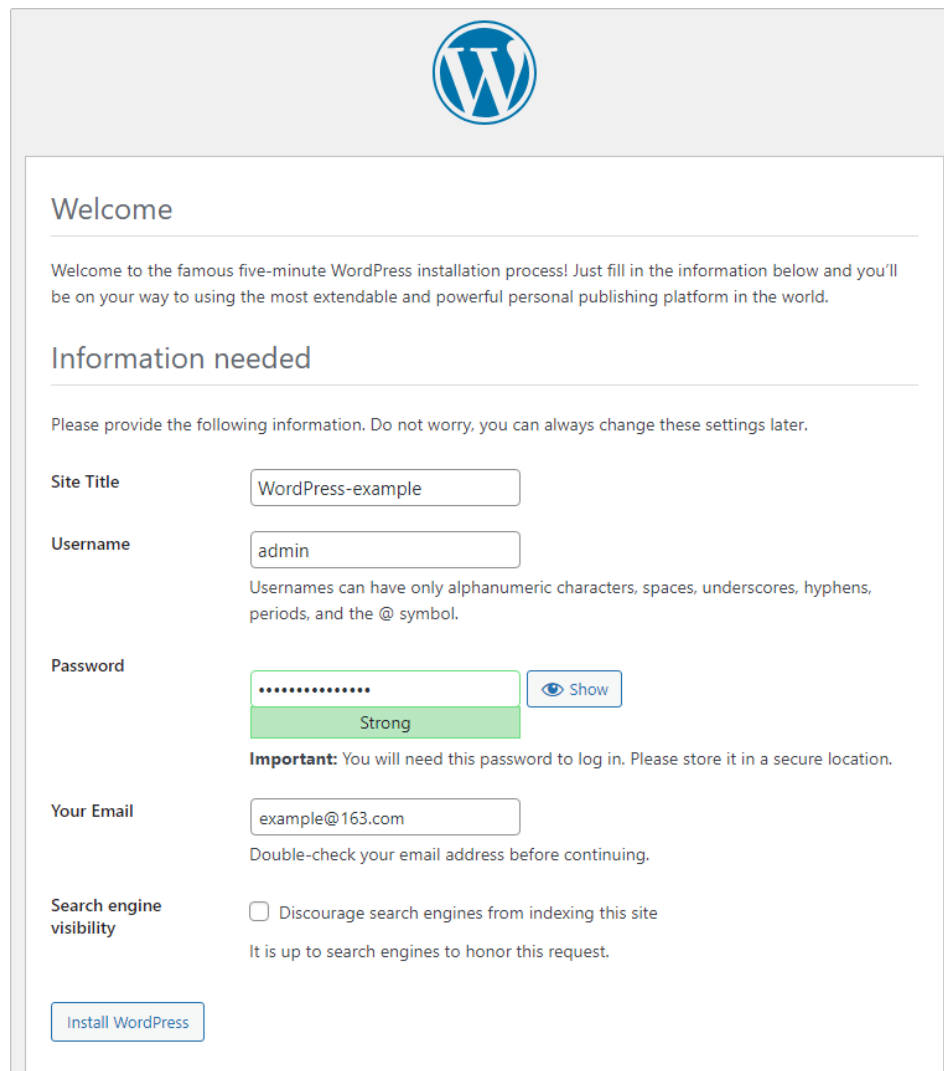
If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure a Security Group](#).
 - The dashboard is being started. Try again later.
2. Select the WordPress language and click **Continue**.



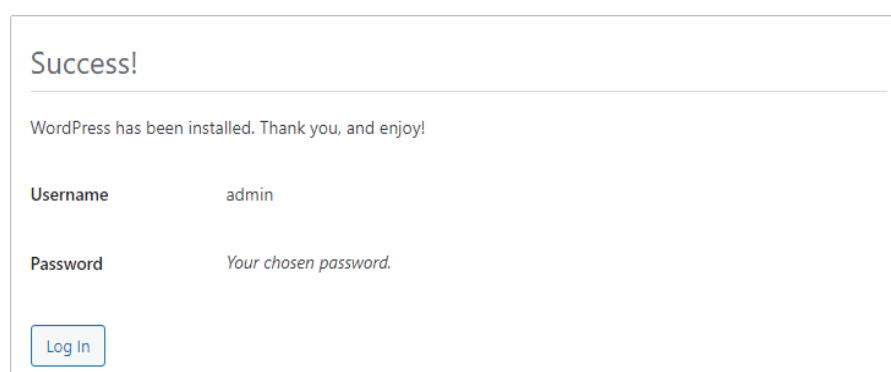
3. Set the website title, WordPress username, password, and email, and click **Install WordPress**.

WordPress does not have an initial username or password. You can customize the username and password during initialization. Keep your website administrator username, password, and email secure. If you forgot the password, you can use this email to reset the password.



The screenshot shows the WordPress installation 'Information needed' form. At the top is the WordPress logo. Below it is a 'Welcome' section with a message: 'Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.' The 'Information needed' section follows, with a note: 'Please provide the following information. Do not worry, you can always change these settings later.' The form contains several fields: 'Site Title' with the value 'WordPress-example'; 'Username' with the value 'admin' and a note that usernames can only have alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol; 'Password' with a masked field '.....', a 'Show' button, and a green 'Strong' password strength indicator, accompanied by an 'Important' note: 'You will need this password to log in. Please store it in a secure location.'; 'Your Email' with the value 'example@163.com' and a note to double-check the email address; and 'Search engine visibility' with an unchecked checkbox for 'Discourage search engines from indexing this site' and a note that it is up to search engines to honor this request. At the bottom is an 'Install WordPress' button.

4. Enter the username and password and click **Log In**.



The screenshot shows the 'Success!' message after WordPress installation. It says 'WordPress has been installed. Thank you, and enjoy!' Below this, it displays the 'Username' as 'admin' and the 'Password' as 'Your chosen password.' At the bottom is a 'Log In' button.

After WordPress is initialized, you can operate the website on the application dashboard.

Step 5: Operate Websites

This section describes common WordPress operations. For more information, see [WordPress Documentation](#).

Configuring Domain Names

Add and resolve a domain name for the website so that users can use the domain name to access the website.

1. If the domain name is not registered with Huawei Cloud or not hosted on Huawei Cloud DNS, the domain name cannot be resolved. Use either of the following methods to resolve the issue:

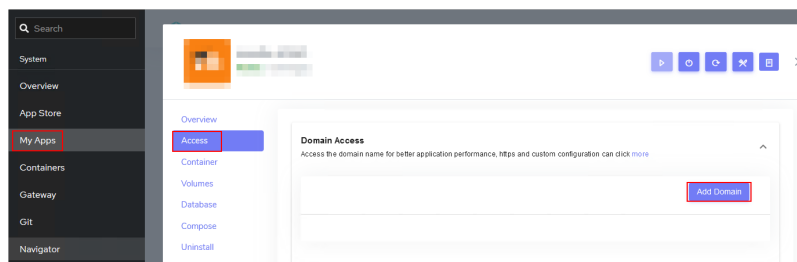
- Contact the DNS service provider to add an A record that maps the domain name to the EIP of the FlexusL instance.
- Use Huawei Cloud DNS servers to resolve the domain name. For details, see [Migrating to Huawei Cloud DNS for Domain Name Resolution](#).

2. Add the domain name on the application O&M page.

- a. In the address bar of a local browser, enter **http://EIP:9000** to log in to the application O&M page.

The username and password for logging in to the dashboard are the **root** user and password of the FlexusL instance. A FlexusL instance does not have an initial password. Reset the password and use it to log in to the dashboard.

- b. Choose **My Apps** and click the App icon.
- c. Choose **Access** and click **Add Domain**.



3. Apply for ICP licensing for the domain name.

To successfully access the server using a domain name, you must license the domain name. Domain name licensing provided by the ICP License Service is free of charge. For details, see [ICP Filing Process](#).

After the domain name is licensed, you can use it to visit the website.

Installing an SSL Certificate for Your Website

If the website is only used for personal development or testing, you can apply for a free SSL certificate (provided by Let's Encrypt) whose validity period is 90 days. If your website is for commercial use, you are advised to install a commercial SSL certificate. After an SSL certificate is installed, HTTPS is used when you access the website using the domain name. The following describes the two methods for installing an SSL certificate for your website.

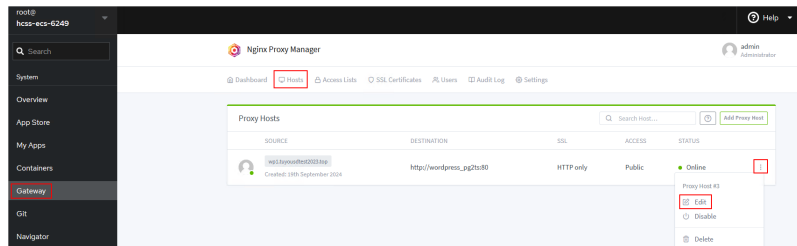
Preparations

Before installing an SSL certificate, initialize the application on the management page and configure the domain name on the application O&M page.

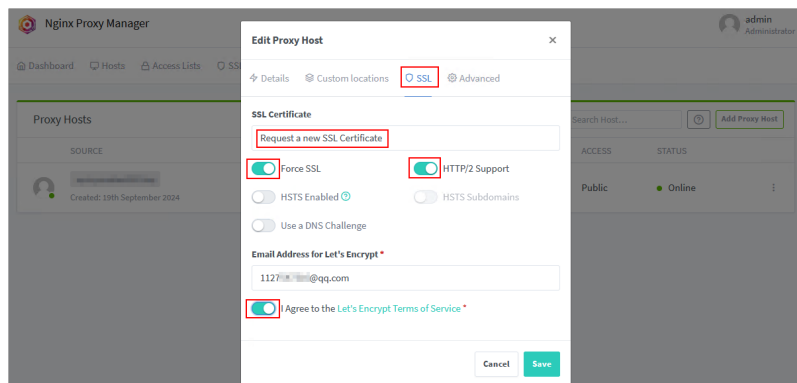
Procedure

- Apply for a free SSL certificate on the application O&M page.
 - a. In the address bar of a local browser, enter **http://EIP:9000** to log in to the application O&M page.

The username and password for logging in to the dashboard are the **root** user and password of the FlexusL instance. A FlexusL instance does not have an initial password. Reset the password and use it to log in to the dashboard.
 - b. Choose **Gateway > Hosts > Proxy Hosts**, click the icon next to the domain name, and click **Edit**.



- c. Select **SSL**, configure the parameters as instructed in the following figure, and click **Save**.

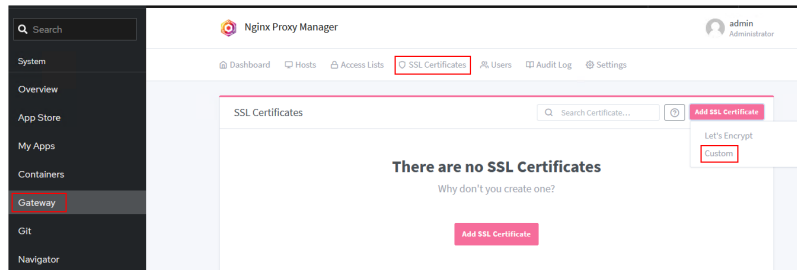


- Install a commercial SSL certificate.

If you have purchased and issued an SSL certificate, perform the following steps to install the certificate for the website. If you have not purchased and issued an SSL certificate, purchase and issue one on Huawei Cloud by referring to [About SCM and SSL Certificate Usage](#), and then perform the following steps to install a certificate for the website.

 - a. In the address bar of a local browser, enter **http://EIP:9000** to log in to the application O&M page.

The username and password for logging in to the dashboard are the **root** user and password of the FlexusL instance. A FlexusL instance does not have an initial password. Reset the password and use it to log in to the dashboard.
 - b. Choose **Gateway > SSL Certificates**, click **Add SSL Certificate**, and select **Custom**.



- c. Enter a name for the certificate, upload the certificate key and certificate, and click **Save**.

Add Custom Certificate
✕

⚠ Key files protected with a passphrase are not supported.

Name *

Certificate Key *

Choose file
Browse

Certificate *

Choose file
Browse

Intermediate Certificate

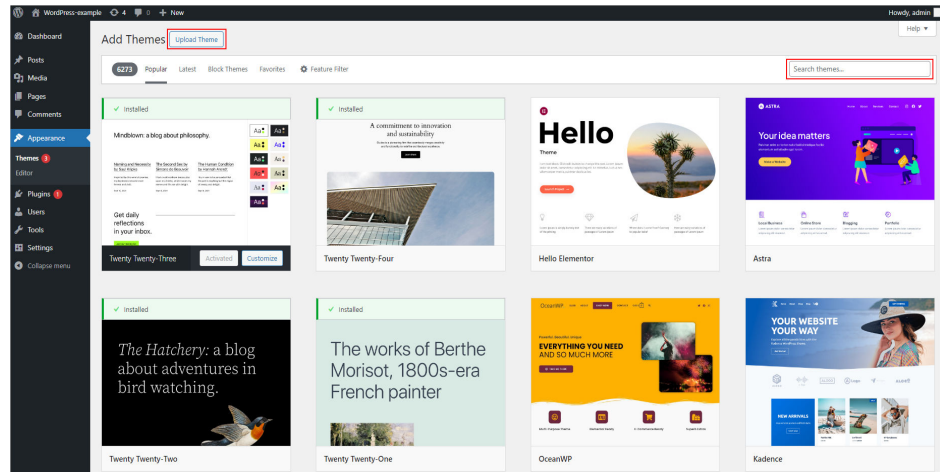
Choose file
Browse

Cancel
Save

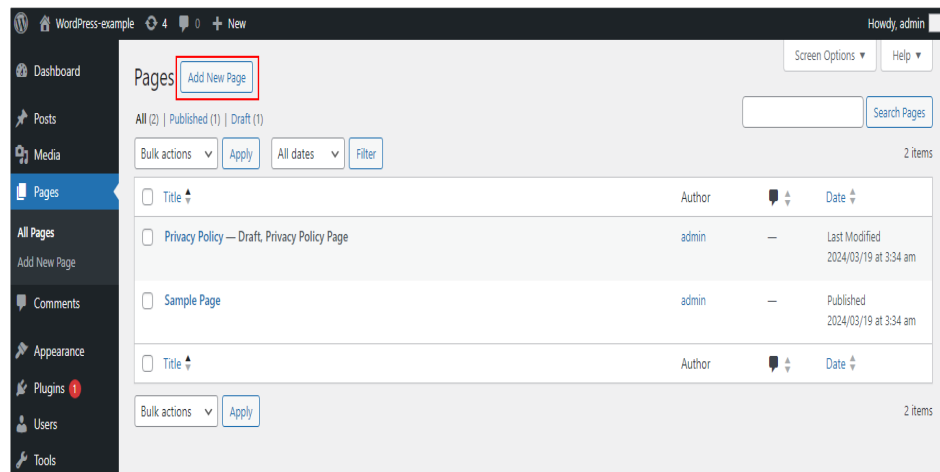
Managing Appearance

WordPress provides a wide range of themes. You can select an appropriate one for your WordPress website. You can change the WordPress theme of your website without changing the website content and structure.

1. Choose **Appearance > Themes** on the WordPress dashboard.
 - You can use the default and active themes, or add new themes.
 - Select a theme from the theme collection provided by WordPress.
 - Click **Upload Theme** and upload third-party themes.



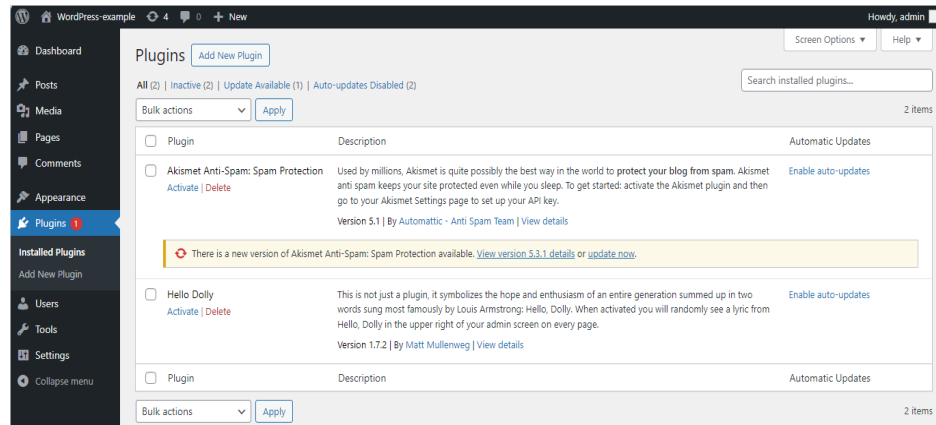
2. After installing a theme, click **Activate**.
3. Choose **Pages > Add New Page** and use the fusion builder provided by the theme to flexibly set up a web page.



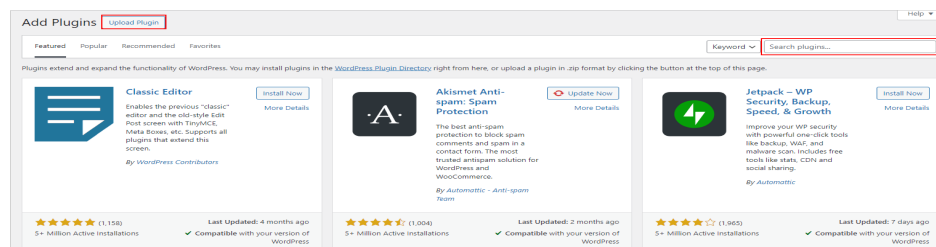
Managing Plugins

WordPress provides many plugins that add more capabilities, choices, and options to your WordPress website.

- Choose **Plugins > Installed Plugins**.
You can view all the plugins that have been installed and their details, such as the developer and functions.



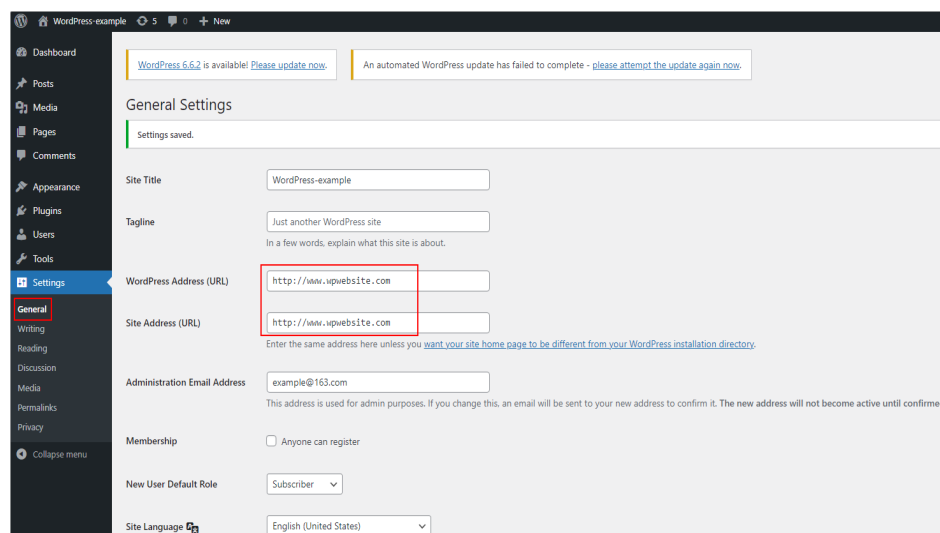
- Choose **Plugins > Add New Plugin** and add plugins.
 - In the upper right corner, select a filter and search for plugins from the WordPress plugin library.
 - Click **Upload Plugin** and select a third-party plugin for installation.



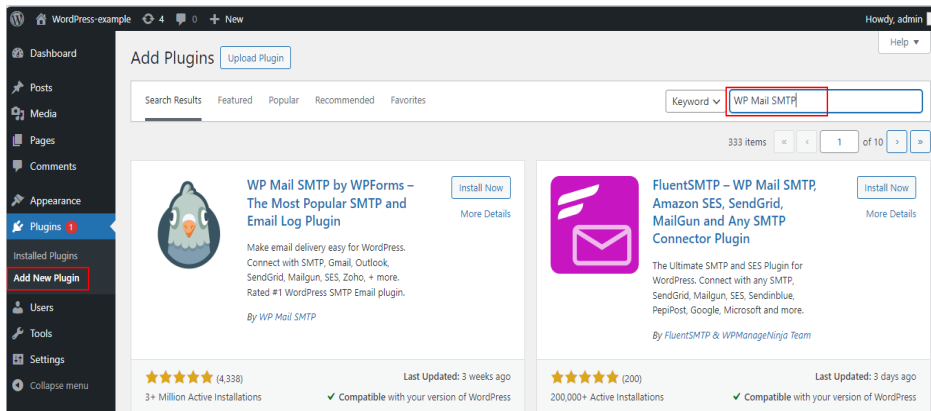
Configuring SMTP

The following uses the 163 email as an example to show how to use the WP Mail SMTP plugin to configure SMTP.

1. Choose **Settings > General** and set the administration email address.



2. Install the WP Mail SMTP plugin.
 - a. On the WordPress dashboard, choose **Plugins > Add New Plugin**.
 - b. Search for the keyword **WP Mail SMTP**. In the displayed result, click **Install Now**. After the installation is complete, click **Activate**.



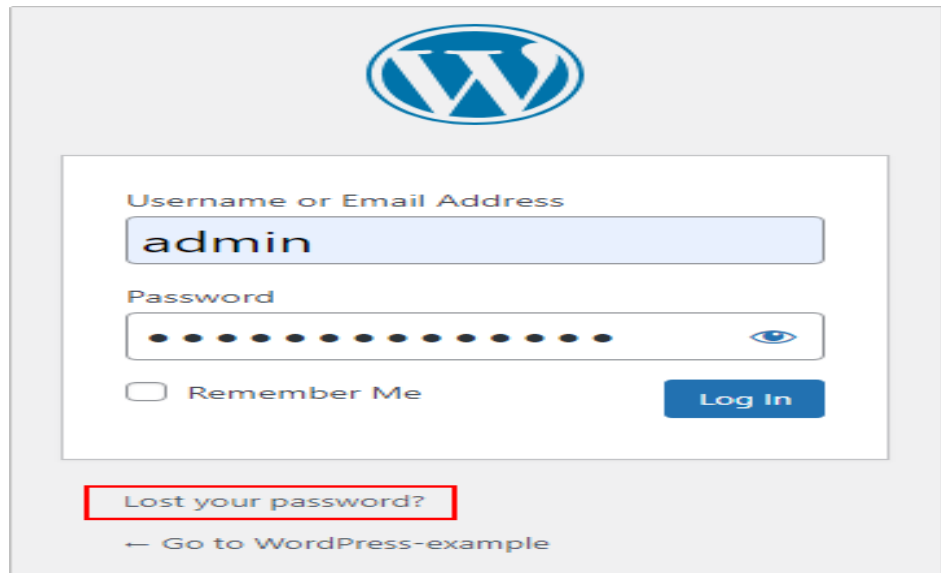
- Go back to the dashboard, configure SMTP, and click **Save Settings**.
The following uses the 163 mailbox as an example to show how to configure a mailbox. If you use another mailbox, specify corresponding parameters.

Parameter	Description
From Email	The email address that emails are sent from, which is the email address that you specify during WordPress installation by default. In this example, the value is <i>example@163.com</i> . You can change the value as needed. NOTE SMTP must be configured for the email address.
From Name	The name that emails are sent from, which can be your website name. The default value is the website title that you specify during WordPress installation. In this example, the value is <i>WordPress-example</i> . You can change the value as needed.
Mailer	Select Other SMTP .
SMTP Host	SMTP host IP address. Enter <i>smtp.163.com</i> in this example.
Encryption	Select SSL .
SMTP Port	Enter <i>465</i> in this example.
Auto TLS	Enable this function.
Authentication	Enable this function.
SMTP Username	Keep it the same as the From Email parameter value: <i>example@163.com</i> .
SMTP Password	Enter the authorization code obtained when configuring SMTP for the email <i>example@163.com</i> . This is not the password of the email <i>example@163.com</i> .

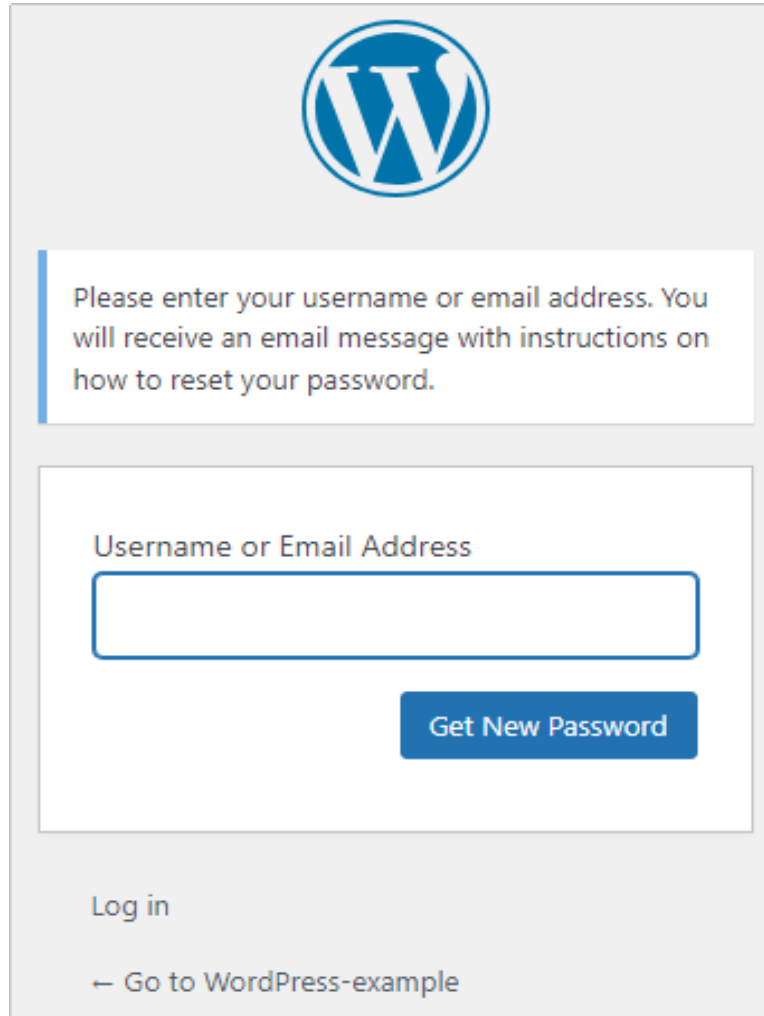
Resetting a Password

If you forgot the WordPress administrator password, you can reset the password via email (SMTP must have been configured for WordPress).

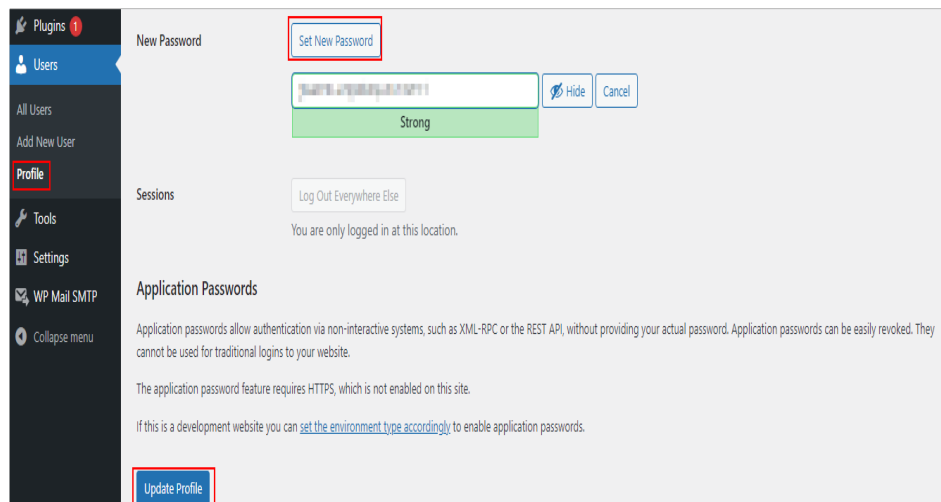
- Resetting a password via email
 - a. On the WordPress login page, click **Lost your password**.



- b. Enter the username or email address and click **Get New Password**. Then a new password will be sent to your email.



- c. On the dashboard, choose **Users > Profile**. On the displayed page, set a new password and click **Update Profile**.



2.3 Using Matomo to Build a Website Traffic Statistics System

Application Scenario

Matomo is a powerful open-source network analysis platform that has full data ownership and ensures that the business complies with General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). Supported By FlexusL, the Matomo application image uses Ubuntu 22.04 and is deployed using Docker. The Nginx, MySQL, phpMyAdmin, and Docker have been preconfigured in the image. You can use this application image to analyze website data.

Resource Planning and Costs

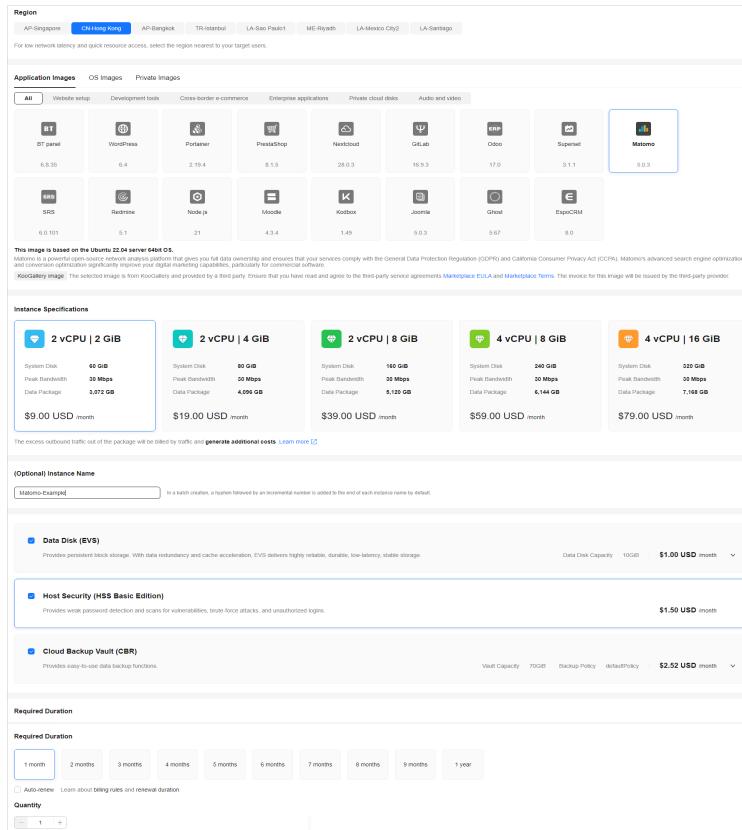
Resource	Configuration	Description
Cloud server	<ul style="list-style-type: none">vCPUs: 2Memory: 2 GiB	Select appropriate instance specifications based on your service requirements.
Image	Matomo	Select the Matomo application image.
Security group	Inbound rule: <ul style="list-style-type: none">Protocol/ Application: TCPPort: 80, 9001Source: 0.0.0.0/0	<ul style="list-style-type: none">80: Specifies the internal forwarding port of application images.9000: Allows external access to the application O&M page.9001: Allows external access to the application dashboard.

Process

Procedure	Description
Step 1: Purchase a FlexusL Instance	Purchase a FlexusL instance and select the Matomo application image.
Step 2: Configure Security Groups	Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.
Step 3: Reset the Password and Log In to the FlexusL Instance	A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance before logging in to it.
Step 4: Initialize Matomo	Install and initialize Matomo.
Step 5: Use Matomo to Monitor Websites	Add tracking code to the websites you want to monitor.

Step 1: Purchase a FlexusL Instance

1. Log in to the FlexusL [console](#) and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Application Image	Matomo	Select the Matomo application image.
Instance Specifications	2 vCPUs 2 GiB memory and 60 GiB system disk	Select instance specifications as needed.
Instance Name	Matomo-Example	Customize an instance name that is easy to identify, for example, Matomo-Example.

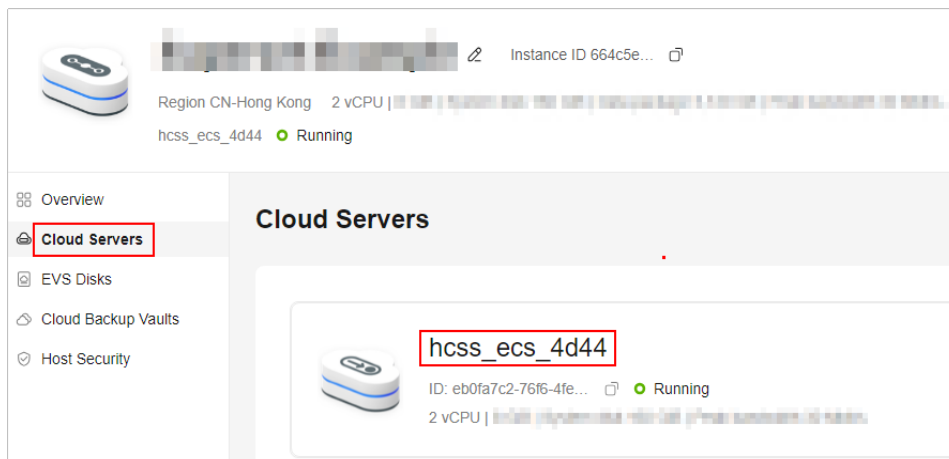
Parameter	Example	Description
(Optional) Associated Services	<ul style="list-style-type: none">• Data disk: 10 GiB• Host security• Cloud backup vault: 70 GiB	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure Security Groups

Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.

The following figure only displays common rules. You can add more rules as needed.

Table 2-3 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of application images
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

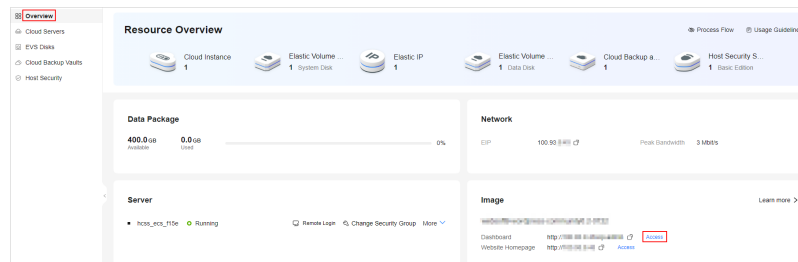
Step 3: Reset the Password and Log In to the FlexusL Instance

This section describes how to log in to a FlexusL instance. A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance before logging in to it.

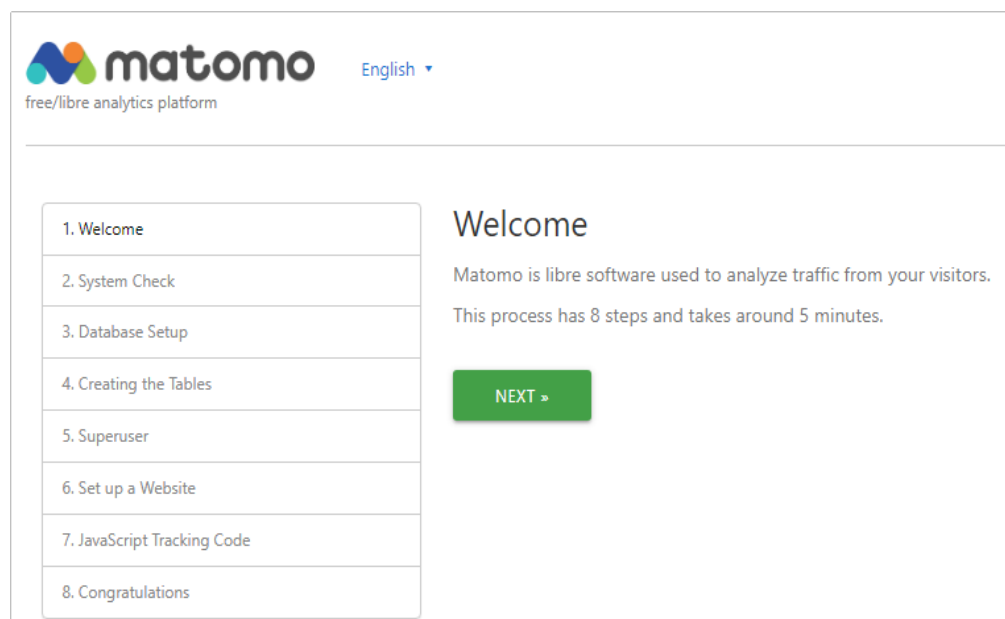
1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard and check whether the application has been up and running. If yes, go to the next step.

NOTICE

Wait for several minutes until the image with the pre-installed application is up and running. Then, you can perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the initial password may become invalid and you cannot log in to the application dashboard.

Figure 2-6 Entry to the application dashboard

After the application is started, the initialization wizard page of the dashboard is displayed, as shown in [Figure 2-7](#).

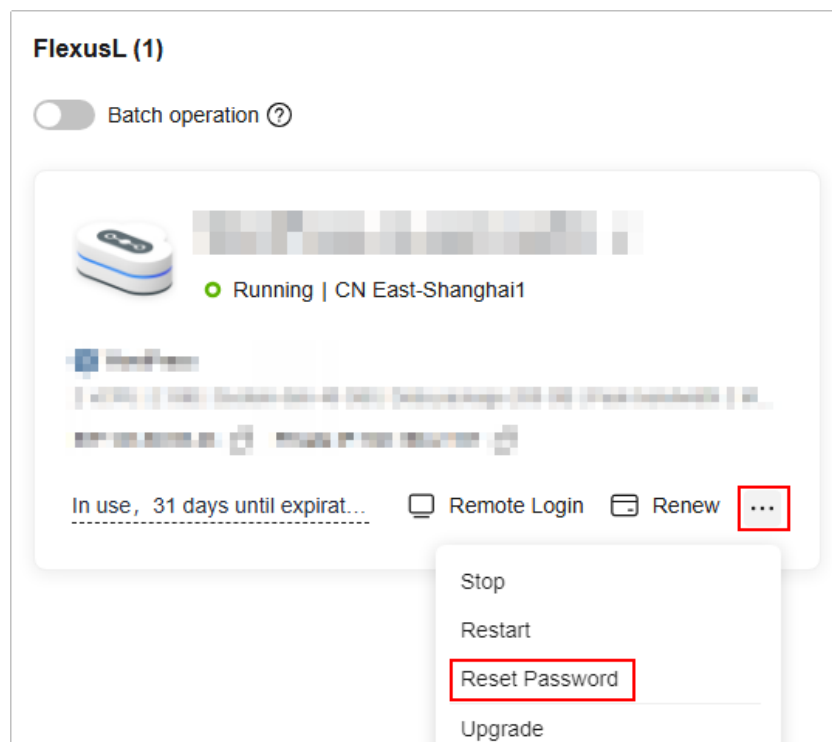
Figure 2-7 Initialization wizard page of the Matomo dashboard**NOTE**

If the dashboard is not properly displayed, check the following causes:

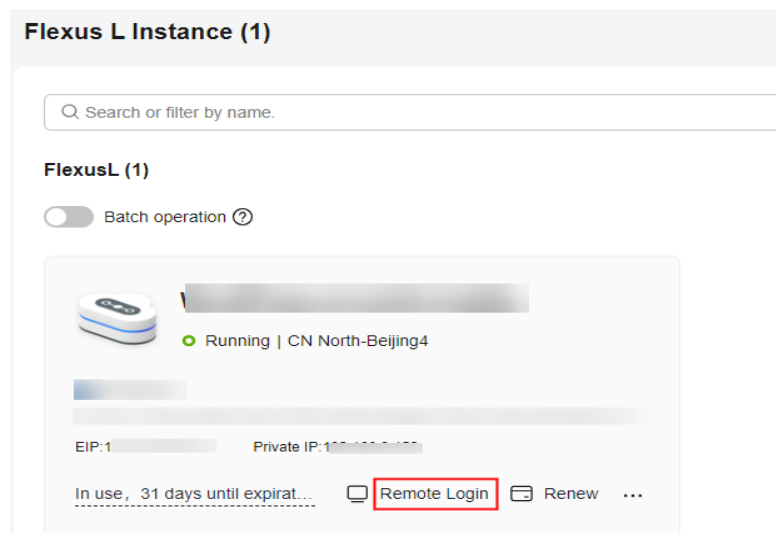
- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
 - The dashboard is being started. Try again later.
2. Locate the resource card and choose **...** > **Reset Password** to reset the password.

A FlexusL instance does not have an initial password. Set a password for the FlexusL instance before logging in to it. For details, see [Resetting the Password for a FlexusL Instance](#).

Figure 2-8 Resetting a password



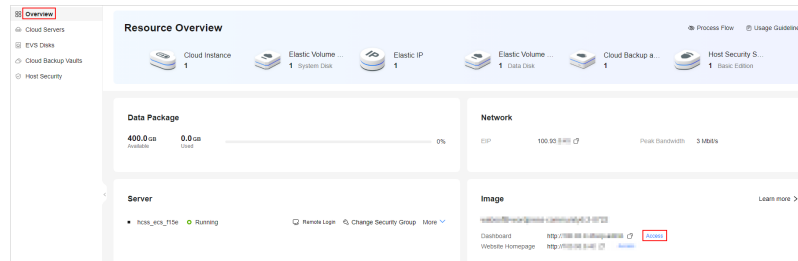
3. Locate the target instance and click **Remote Login** and enter the username and password as prompted to log in to the FlexusL instance. The username is **root**, and the password is the one set in 2.



Step 4: Initialize Matomo

Application images use code-based Ubuntu. They provide graphical user interfaces to make your operations easier. You need to initialize the application dashboard upon the first login. Then you can directly log in to the dashboard from the FlexusL console afterwards.

1. On the **Overview** page, click **Access** in the **Dashboard** field in the **Image** area.



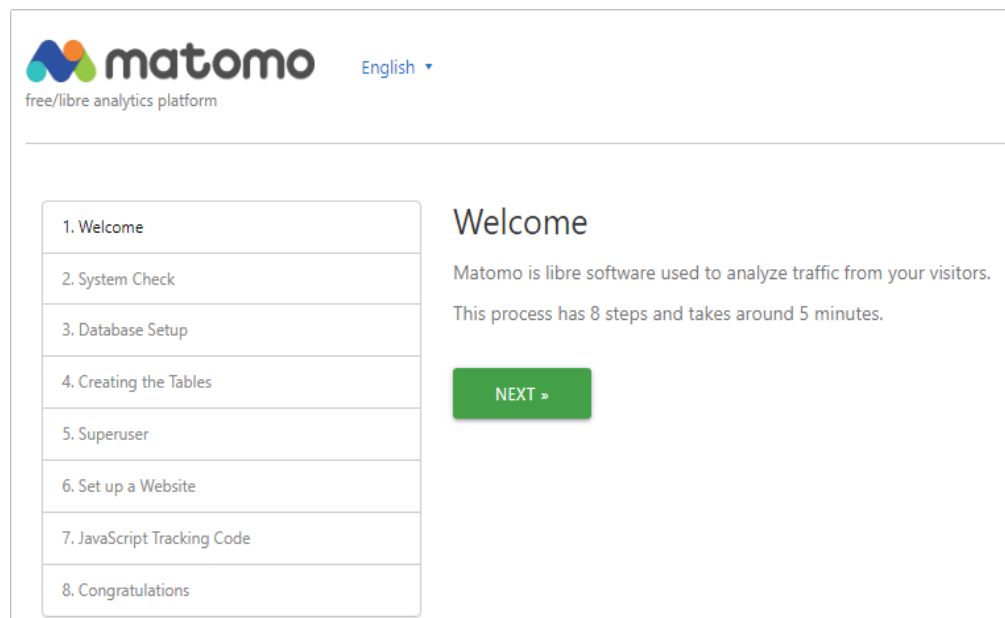
NOTE

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
- The dashboard is being started. Try again later.

2. Click **NEXT**.

Figure 2-9 Initialization wizard page of the Matomo dashboard



3. Wait until Matomo completes the system check and click **NEXT**.
Matomo automatically checks whether the server meets the requirements for installing Matomo and displays the check result for each item.
4. Set up the MySQL database and click **NEXT**.
The MySQL database and a default database account have been preset in Matomo. The information about the default database account is automatically obtained. Retain the default settings and click **NEXT**.
5. After Matomo automatically creates data tables, click **NEXT**.
6. On the **Superuser** page, set the username, password, and email address of the Matomo administrator, and click **NEXT**.
The super user is the user that you created when you installed Matomo. Each Matomo has only one super user who has the highest permissions. Keep the username and password of the super user secure.

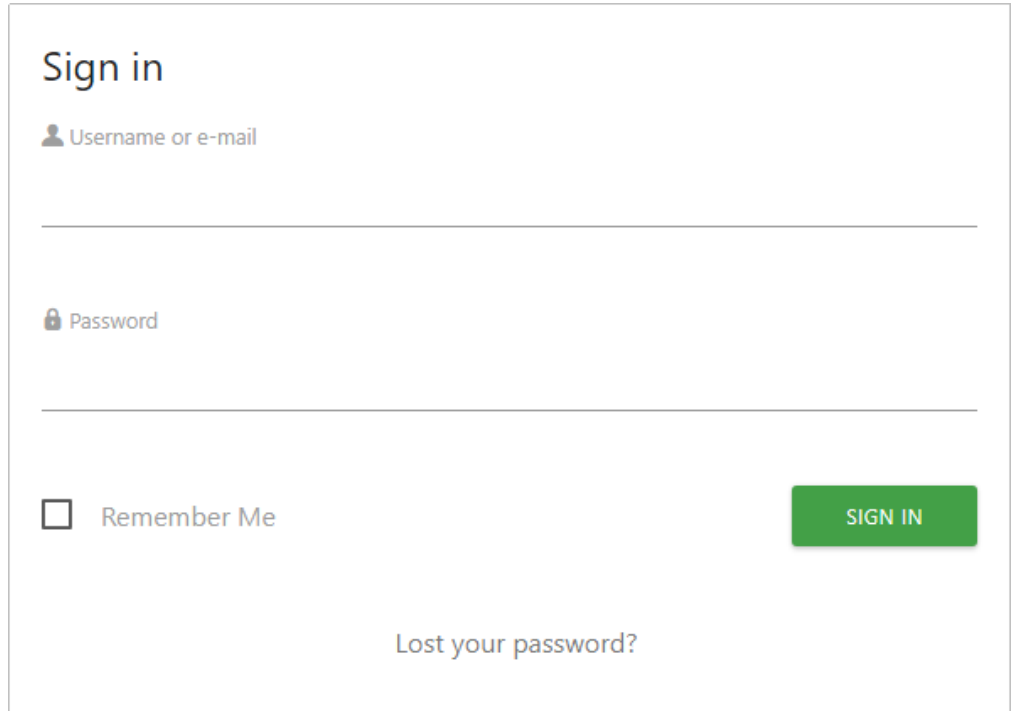
The screenshot shows the 'Superuser' creation page in Matomo. On the left is a progress bar with steps 1 through 8, where '5. Superuser' is currently selected. The main content area is titled 'Superuser' and contains a 'Superuser login' section with three input fields: 'Password', 'Password (repeat)', and 'Email'. Below these fields are two checkboxes: 'subscribe to our newsletter to receive regular information about Matomo.' and 'send me info on Professional services and products for Matomo'. A green 'NEXT >' button is at the bottom. A grey informational box on the right states: 'Your email address will only be used to send you the newsletter. It is shared with Mad Mimi to do so, but the third-party provider may change. We will not share your email with anyone else or use your it for any other purpose. Unsubscribe at any time. The [privacy policy](#) has more info.'

7. On the **Set up a Website** page, add the name and URL of the first website you want to track and analyze with Matomo and click **NEXT**.

You can add more websites to track later.

The screenshot shows the 'Set up a Website' page in Matomo. On the left is a progress bar with steps 1 through 8, where '6. Set up a Website' is currently selected. The main content area is titled 'Set up a Website' and features a green success message: 'Superuser created.' Below this is the instruction: 'Please set up the first website you would like to track and analyse with Matomo:'. The form includes fields for 'Website name', 'Website URL' (with 'https://example.org' entered), 'Website timezone', 'Select a city' (a dropdown menu), 'Ecommerce', and 'Not an Ecommerce site' (a dropdown menu). A green 'NEXT >' button is at the bottom. A note at the bottom reads: 'Note: Once Matomo is fully installed, you can add more websites to track.'

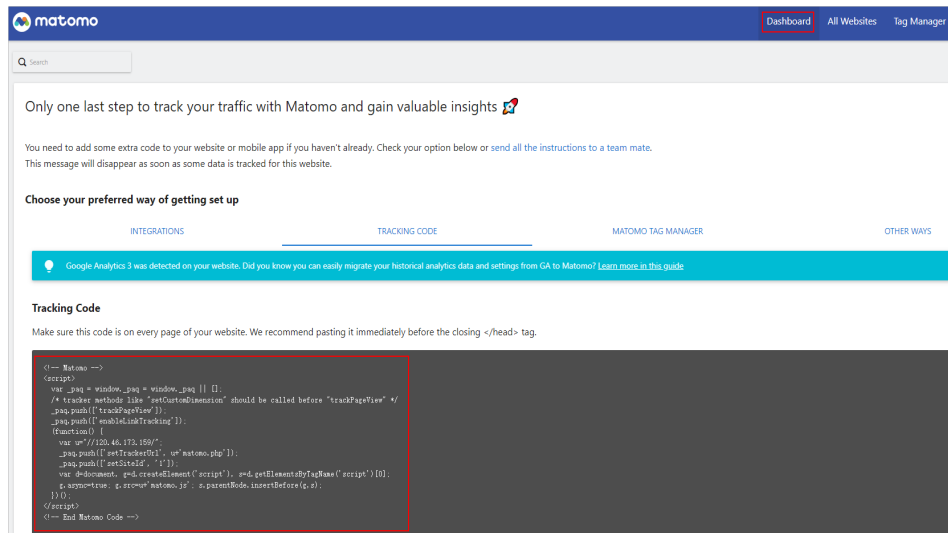
8. Learn about the JavaScript tracking code and click **NEXT**.
To track your web traffic with Matomo, you need to make sure that some extra code is added to each of your webpages. Matomo automatically generates a JavaScript tracking code. After the installation is complete, you can check the tracking code in the **Tracking Code** admin section.
9. After the initialization configurations are complete, click **Continue to Matomo**.
10. Enter the username and password of the super user and click **SIGN IN**.



After the Matomo application is initialized, you can monitor websites on the application dashboard.

Step 5: Use Matomo to Monitor Websites

1. On the dashboard, click the **TRACKING CODE** tab and copy the tracking code in the **Tracking Code** area.

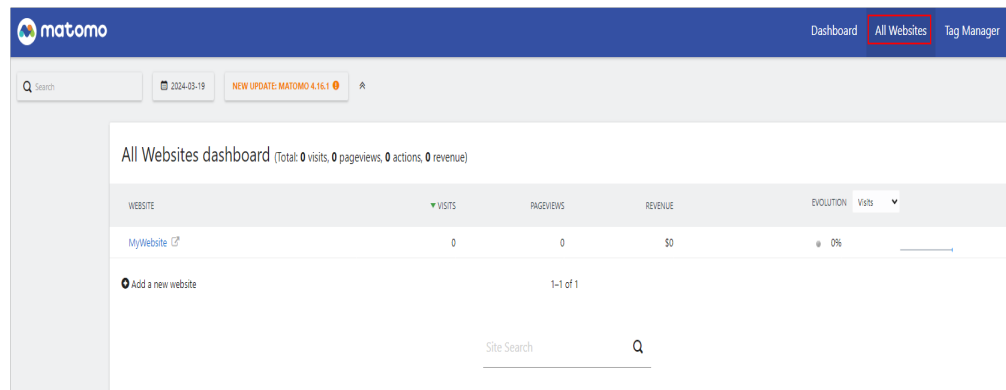


2. Copy the tracking code to each page of the website you want to monitor. Matomo can collect real-time analysis data of the website with the tracking code.

NOTE

For details about how to install the Matomo tracking code, see [official documentation](#).

3. Select **All Websites** to view the access to the monitored websites.



2.4 Using Odoo to Build an ERP System

Application Scenario

Odoo is an open-source ERP/CRM software that integrates a comprehensive suite of applications for managing all aspects of your business, including procurement, inventory, finance and accounting, marketing, manufacturing, human resources management, service support, e-commerce, and website building, achieving fully automated service processes. Supported By FlexusL, the Odoo application image uses Ubuntu 22.04 and is deployed using Docker. The Nginx, pgAdmin, and Docker have been preconfigured in the image. This section describes how to use Odoo to build an ERP system.

Resource Planning and Costs

This practice uses the following resource planning as an example. You can adjust it as required.

Resource	Configuration	Description
Cloud server	<ul style="list-style-type: none"> vCPUs: 2 Memory: 2 GiB 	Select appropriate instance specifications based on your service requirements.
Image	Odoo	Select the Odoo application image.
Security group	Inbound rule: <ul style="list-style-type: none"> Protocol/ Application: TCP Port: 80,9001 Source: 0.0.0.0/0 	<ul style="list-style-type: none"> 80: Specifies the internal forwarding port of application images. 9000: Allows external access to the application O&M page. 9001: Allows external access to the application dashboard.

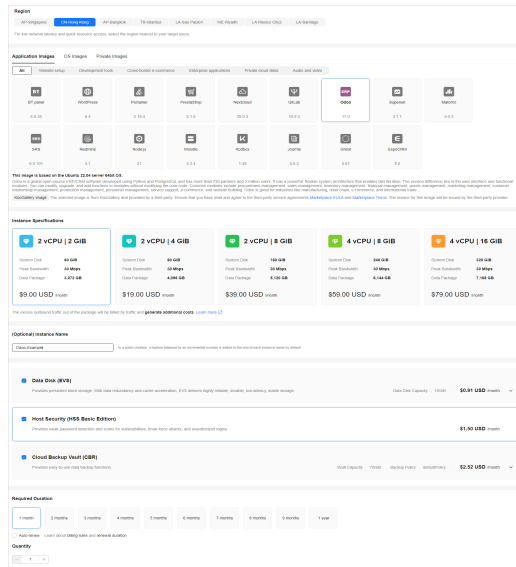
Resource	Configuration	Description
Domain name	wpwebsite.com	<ul style="list-style-type: none">• If the website is only used for personal development or testing, there is no need to add a domain name.• If the website is open to the public, add and resolve a domain name for the cloud server.

Process

Procedure	Description
Step 1: Purchase a FlexusL Instance	Purchase a FlexusL instance and select the Odoo application image.
Step 2: Configure Security Groups	Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.
Step 3: Reset the Password and Log In to the FlexusL Instance	A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance before logging in to it.
Step 4: Initialize Odoo	Log in to Odoo and create databases.
Step 5: Deploy Odoo	On the dashboard, perform the following operations: <ul style="list-style-type: none">• Configure general settings• Obtain administrator information and technical support• Manage databases

Step 1: Purchase a FlexusL Instance

1. Log in to the FlexusL [console](#) and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Application Image	Odoo	Select the Odoo application image.
Instance Specifications	2 vCPUs 2 GiB memory and 60 GiB system disk	Select instance specifications as needed.
Instance Name	Odoo-Example	Customize an instance name that is easy to identify, for example, Odoo-Example.
(Optional) Associate Services	<ul style="list-style-type: none"> Data disk: 10 GiB Host security Cloud backup vault: 70 GiB 	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.

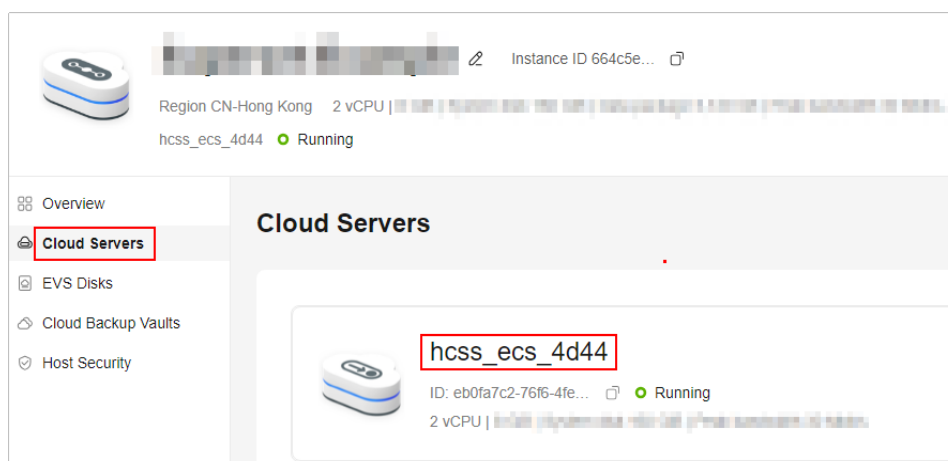
Parameter	Example	Description
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure Security Groups

Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.

The following figure only displays common rules. You can add more rules as needed.

Table 2-4 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of application images
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

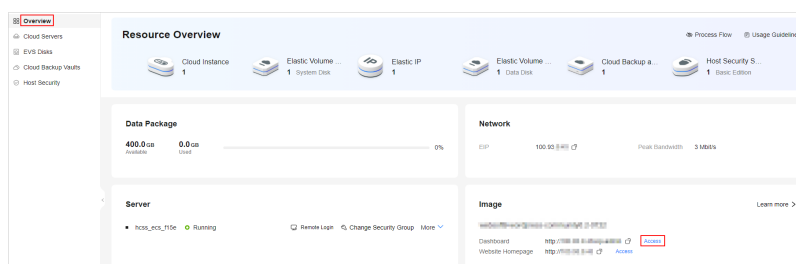
Step 3: Reset the Password and Log In to the FlexusL Instance

This section describes how to log in to a FlexusL instance. A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance before logging in to it.

1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard and check whether the application has been up and running. If yes, go to the next step.

NOTICE

Wait for several minutes until the image with the pre-installed application is up and running. Then, you can perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the initial password may become invalid and you cannot log in to the application dashboard.

Figure 2-10 Entry to the application dashboard

After the application is started, the initialization wizard page of the dashboard is displayed, as shown in [Figure 2-11](#).

Figure 2-11 Initialization wizard page of the Odoo dashboard

Warning, your Odoo database manager is not protected. To secure it, we have generated the following master password for it:

6mjb-9h9u-2k78

You can change it below but be sure to remember it, it will be asked for future operations on databases.

Master Password: example

Database Name: Database1

Email: example@163.com

Password:

Phone number:

Language: Chinese (Simplified) / [redacted]

Country: China

Demo data:

[Create database](#) [or restore a database](#)

NOTE

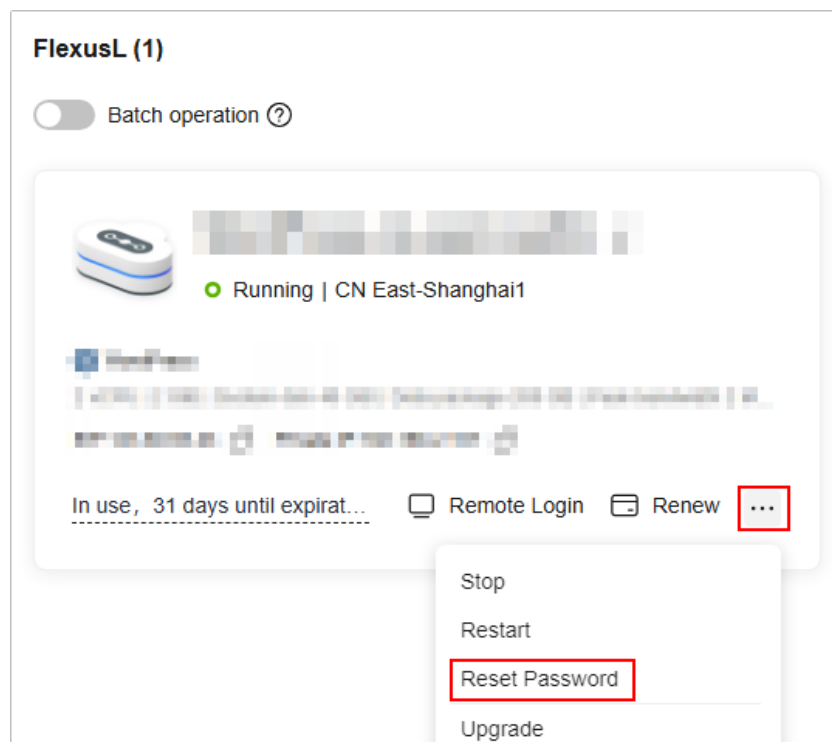
If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
- The dashboard is being started. Try again later.

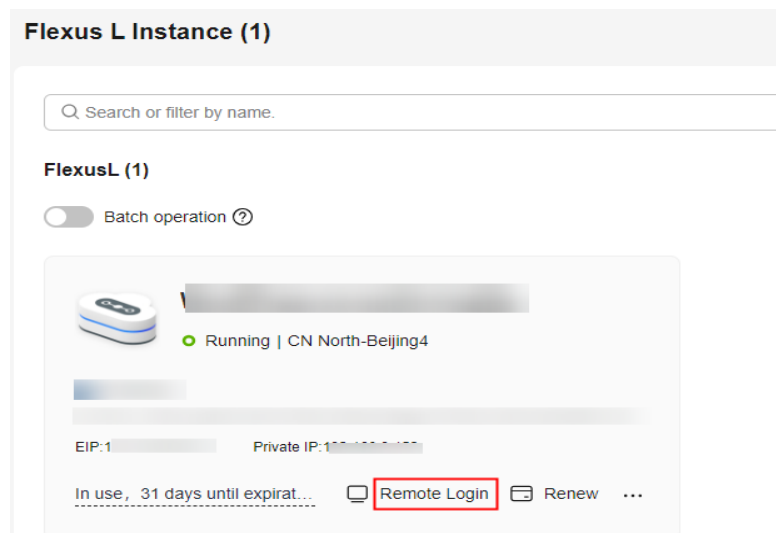
2. Locate the resource card and choose **Reset Password** to reset the password.

A FlexusL instance does not have an initial password. Set a password for the FlexusL instance before logging in to it. For details, see [Resetting the Password for a FlexusL Instance](#).

Figure 2-12 Resetting a password



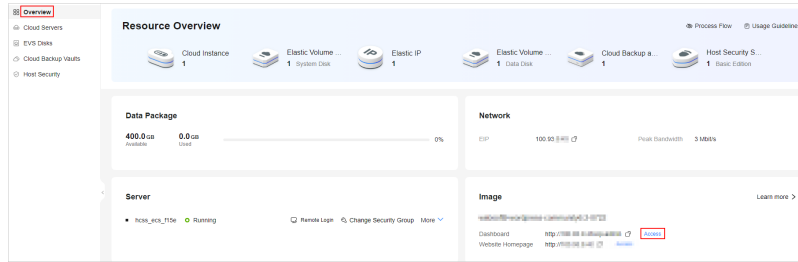
3. Locate the target instance and click **Remote Login** and enter the username and password as prompted to log in to the FlexusL instance. The username is **root**, and the password is the one set in 2.



Step 4: Initialize Odoo

Application images use code-based Ubuntu. They provide graphical user interfaces to make your operations easier. You need to initialize the application dashboard upon the first login. Then you can directly log in to the dashboard from the FlexusL console afterwards.

1. On the **Overview** page, click **Access** in the **Dashboard** field in the **Image** area.



NOTE

- If the dashboard is not properly displayed, check the following causes:
- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
 - The dashboard is being started. Try again later.
2. Configure the parameters and click **Create database**.
If you have had a **backup** database on your local device, click **or restore a database**.

Figure 2-13 Initialization wizard page of the Odoo dashboard

Warning, your Odoo database manager is not protected. To secure it, we have generated the following master password for it:

6mjb-9h9u-2k78

You can change it below but be sure to remember it, it will be asked for future operations on databases.

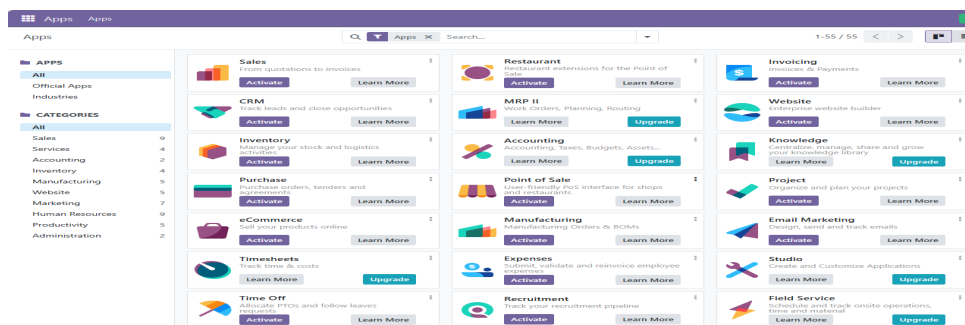
Master Password	<input type="text" value="example"/>
Database Name	<input type="text" value="Database1"/>
Email	<input type="text" value="example@163.com"/>
Password	<input type="password" value="....."/>
Phone number	<input type="text"/>
Language	Chinese (Simplified) / <input type="text"/>
Country	China
Demo data	<input checked="" type="checkbox"/>

[or restore a database](#)

Table 2-5 Parameter descriptions

Parameter	Description
Master Password	The system automatically generates a database master password. You can change it but be sure to remember it. NOTE The database master password will be asked for future operations on databases, so please keep it safe.
Database Name	Specifies a database name.
Email/Password	Specifies the email address and password for the administrator to log in to Odoo. Please keep it safe.
Phone number	Specifies the telephone number of the administrator.
Language	Specifies the language you want to use on the management console.
Country	Specifies the country or region where you are located.
Demo data	After this option is selected, data samples are automatically generated for the created database.

3. Enter the email address and password, and click **Log in**.
The management console is displayed.




After the Odoo application is initialized, you can deploy your applications on the dashboard.

Step 5: Deploy Odoo

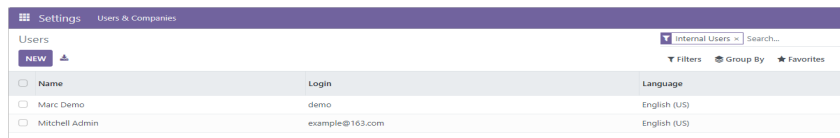
This section describes some basic operations of Odoo. For more information, see [Odoo Documentation](#).

General Settings

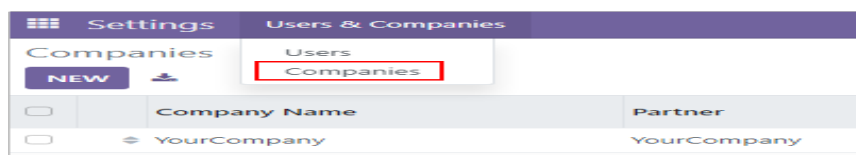
1. Click  in the upper left corner and choose **Settings**.
2. Add a user.

- a. Click **New** in the upper left corner.
- b. After the user is added, click the username to view or modify the username, email address, access permissions, and preferences.

The email address must be unique. If you enter a name that already exists, the message indicating the operation cannot be completed because you cannot have two users with the same login will be displayed.



3. Add a company.
 - a. Choose **User & Companies > Companies**, click **New**, and enter the company name and general information.

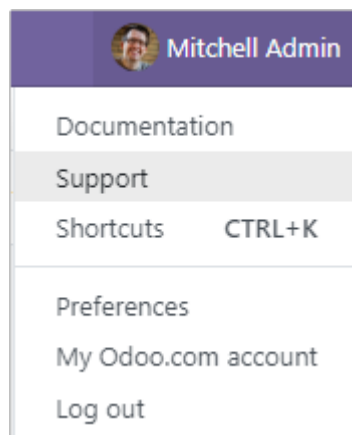


- b. Click **New** in the upper right corner.
After the company is added, you can click the company name to view or modify the basic information about the company.

Obtaining Administrator Information and Technical Support

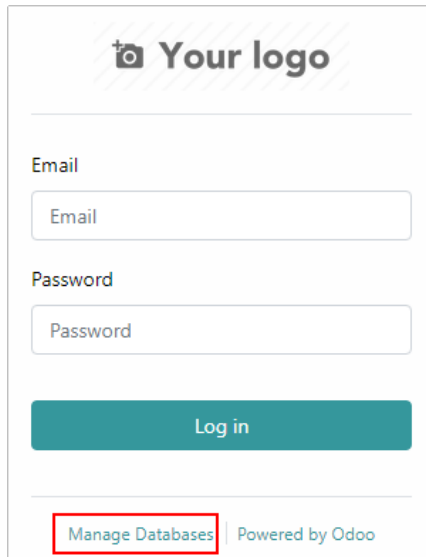
Click the administrator avatar in the upper right corner.

- Click **Documentation** to obtain the official Odoo guide.
- Click **Support** to go to the Odoo official website and learn more about Odoo products.
- Press **Shortcuts CTRL+K** to set the shortcut key.
- Click **Preferences** and set administrator preferences and account security information.
- Click **My Odoo.com account** to go to the Odoo login page.



Managing Databases

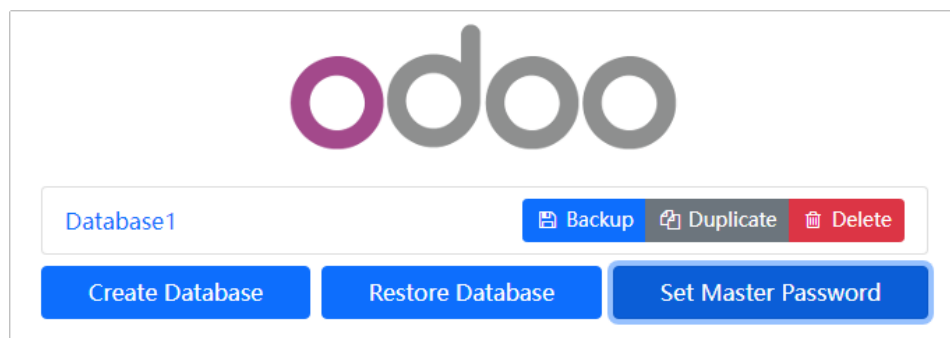
On the Odoo login page, click **Manage Databases** to access the Odoo database manager.



NOTE

You can access the Odoo login page:

- From the FlexusL management console. For details, see [1](#).
- By selecting the administrator avatar in the upper right corner and clicking **Log out**, if you have logged in to Odoo.
- (Optional) Set Master Password
If you did not change the database master password when **initialing Odoo**, you can reset a master password that is easy to remember. The master password is required when you create, delete, dump, or restore databases. Please keep it safe.
 - a. Click **Set Master Password** to set a new master password.



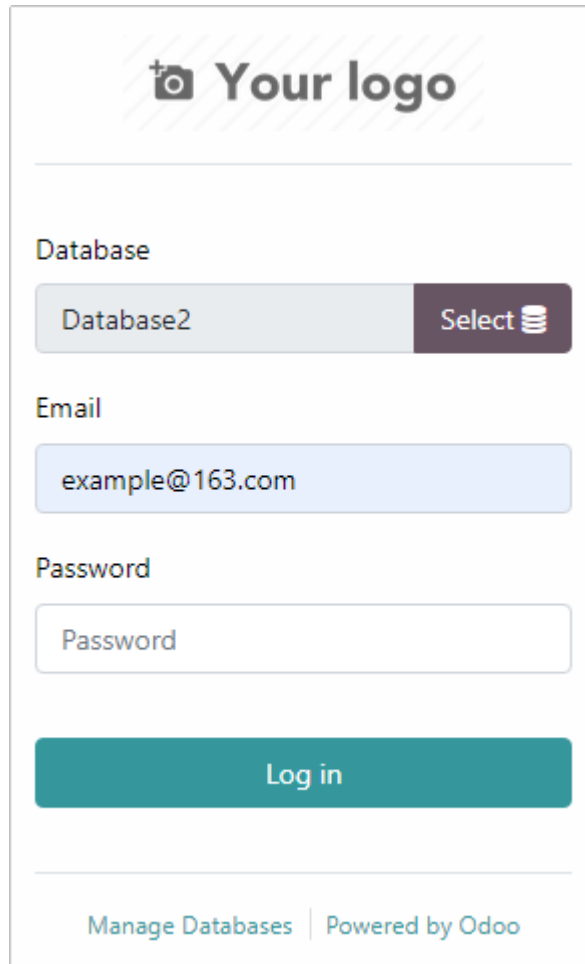
- b. Click **Continue** to save the new master password.
- Create Database
You can add multiple companies on Odoo. Each database means a company. Multiple companies can use Odoo with different accounts and do not interfere with each other.
 - a. Click **Create Database** and set basic information.

The screenshot shows a 'Create Database' dialog box with the following fields and values:

- Master Password: [Redacted]
- Database Name: Database2
- Email: example@163.com
- Password: [Redacted]
- Phone number: [Empty]
- Language: English (US)
- Country: Hong Kong
- Demo data:

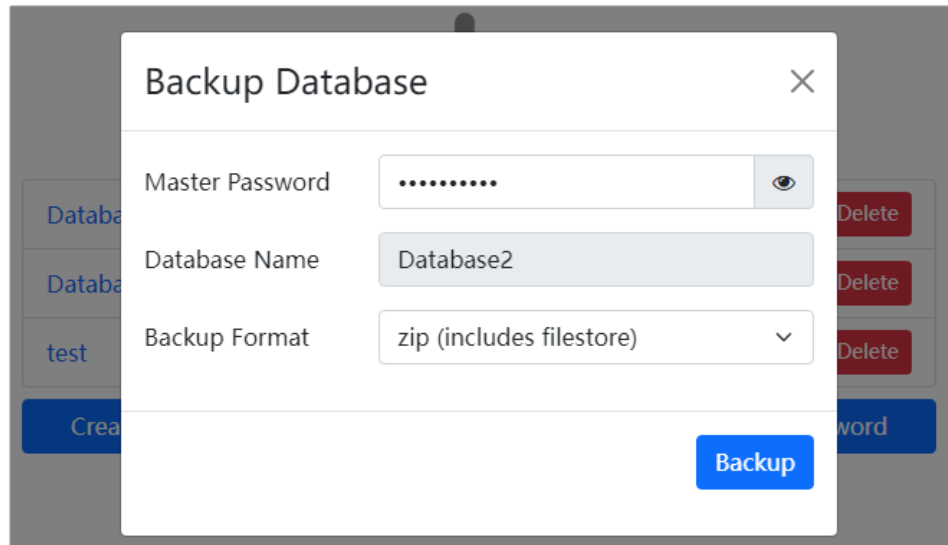
At the bottom right, there is a blue 'Continue' button. Below the form, there is a note: 'To enhance your experience, some data may be sent to Odoo online services. See our [Privacy Policy](#).'

- b. Click **Continue**.
- c. Click **Select**, select **Database2**, and enter the email and password.



The screenshot shows a web interface for database management. At the top, there is a placeholder for a logo with the text "Your logo" and a camera icon. Below this, the "Database" section shows "Database2" selected, with a "Select" button and a database icon. The "Email" field contains "example@163.com". The "Password" field is empty and labeled "Password". A large teal "Log in" button is positioned below the password field. At the bottom, there are links for "Manage Databases" and "Powered by Odoo".

- d. Click **Log in** to log in to the management page of Database2.
 - Backup Database
 - a. On the database management page, click **Backup**.
 - b. On the **Backup Database** page, enter the master password, select a backup format, and click **Backup**.
- After the backup is completed, the system will automatically download the database backup file.



- Duplicate Database
The data of a company can be duplicated and used as the data of a new enterprise.
 - a. On the database management page, click **Duplicate**.
 - b. Enter the master password, set a new database name, and click **Continue**.
After the duplication is successful, the duplicated database will be displayed in the database management column.
- Restore Database
After a database is deleted, it can be restored using backup data.
 - a. Click **Restore Database**.
 - b. Enter the master password, select the backup file, set the database name, and click **Continue**.
After the restoration is successful, the restored database will be displayed in the database management column.

2.5 Using Moodle to Build an Online Learning System

Application Scenario

Moodle is an open-source online education system for global users and can be used for online learning. The Moodle application image uses the Ubuntu 22.04 and is deployed using Docker. The Moodle application and the required operating environment have been preconfigured. This section describes how to install and deploy a Moodle application.

Resource Planning and Costs

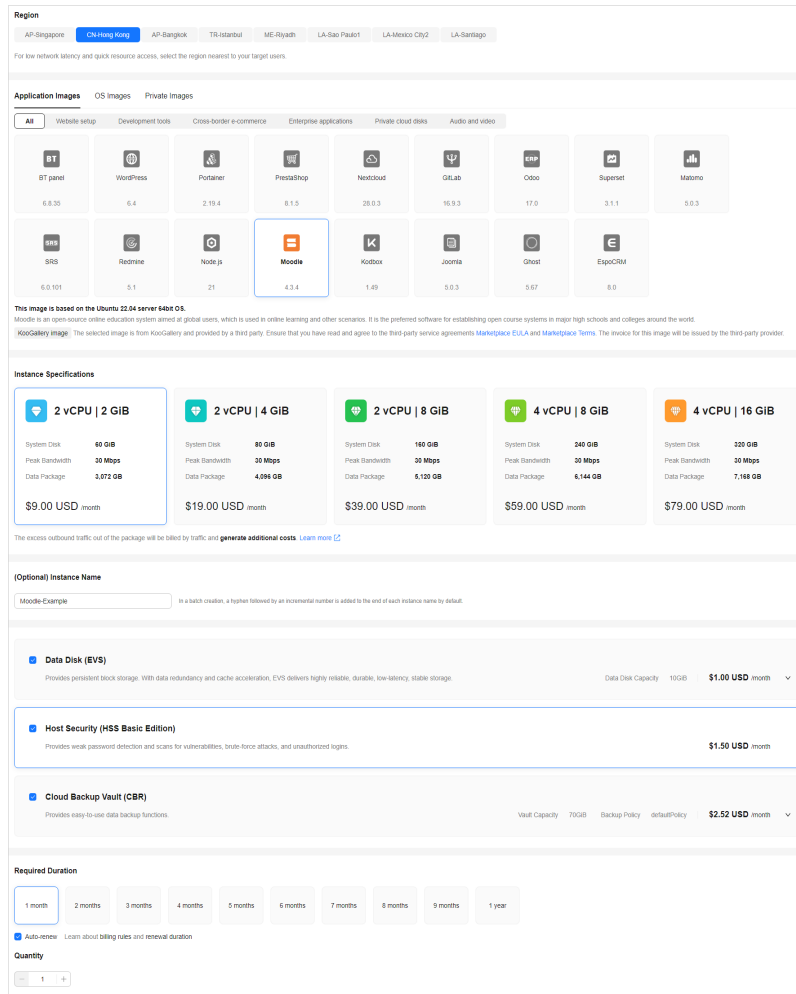
Resource	Configuration	Description
Cloud server	<ul style="list-style-type: none">vCPUs: 2Memory: 2 GiB	Select appropriate instance specifications based on your service requirements.
Image	Moodle	Select the Moodle application image.
Security group	Inbound rule: <ul style="list-style-type: none">Protocol/ Application: TCPPort: 80, 443, 9001, 9000Source: 0.0.0.0/0	<ul style="list-style-type: none">80: Specifies the internal forwarding port of an application.443: Allows HTTPS traffic to FlexusL instances.9001: Allows external access to the application dashboard.9000: Allows external access to the application O&M page.

Process

Procedure	Description
Step 1: Purchase FlexusL Instances	Purchase a FlexusL instance and select the Moodle application image.
Step 2: Configure Security Groups	Add inbound security group rules to allow traffic from ports 80, 443, 9000, and 9001 to access the application.
Step 3: Reset a Password	A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance.
Step 4: Initialize Moodle.	The image application dashboard needs to be initialized only when you log in for the first time.
Step 5: Deploy an Application	Deploy an application on the visualization application management page.

Step 1: Purchase FlexusL Instances

1. Log in to the FlexusL [console](#) and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Application Image	Moodle	Select the Moodle application image.
Instance Specifications	2 vCPUs 2 GiB System disk 60 GiB	Select instance specifications as needed.
Instance Name	Moodle-Example	Customize an instance name that is easy to identify, for example, Moodle-Example.

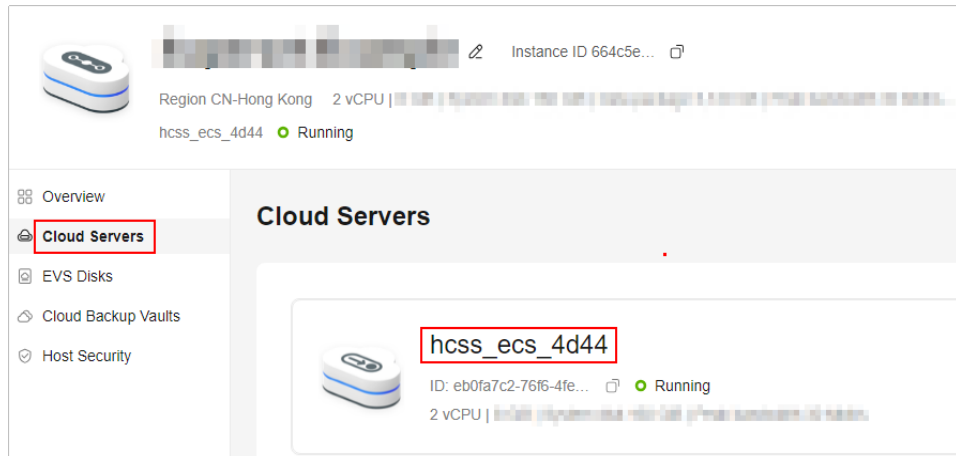
Parameter	Example	Description
(Optional) Associated Service	<ul style="list-style-type: none">• Data Disk: 10 GiB• Host Security• Cloud Backup Vault: 70 GiB	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure Security Groups

Add inbound security group rules to allow traffic from ports 80, 443, 9000, and 9001 to access the application.

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.

The following figure only displays common rules. You can add more rules as needed.

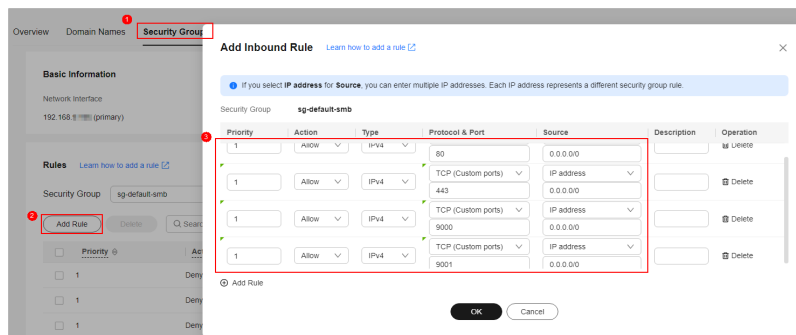


Table 2-6 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of an application.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS traffic to FlexusL instances.
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M page.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

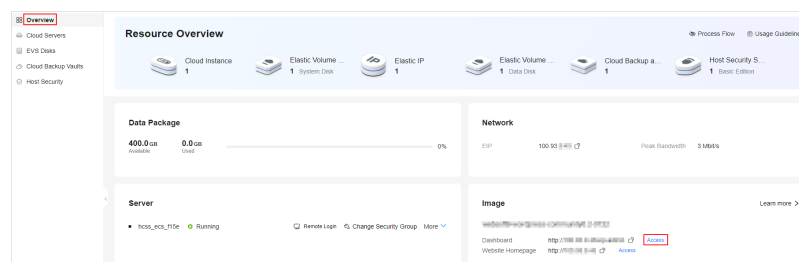
Step 3: Reset a Password

A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for it. The password of the FlexusL instance is also used for [logging in to the O&M page of the application](#).

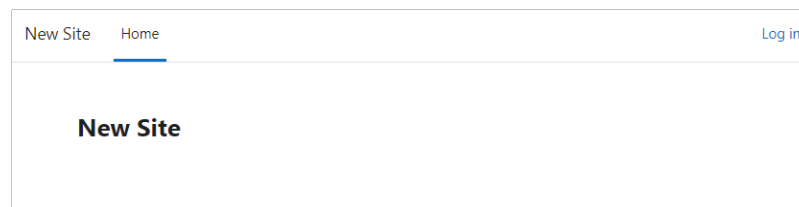
1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard and check whether the application has been up and running. If yes, go to the next step.

NOTICE

Wait for several minutes until the image with the pre-installed application is up and running. Then, you can perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the initial password may become invalid and you cannot log in to the application dashboard.

Figure 2-14 Entry to the application dashboard

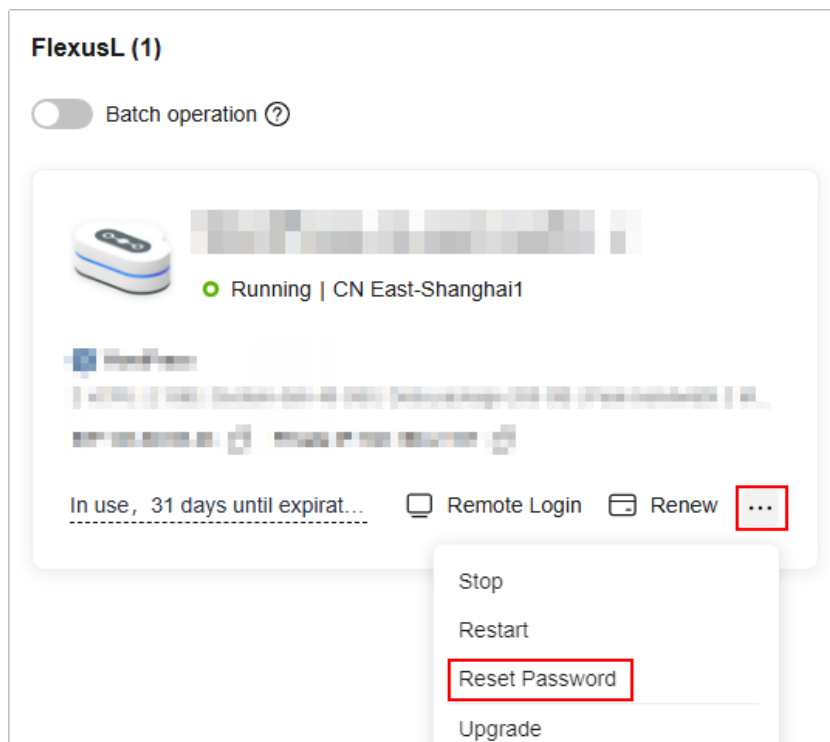
After the application is started, the initialization wizard page of the dashboard is displayed, as shown in [Figure 2-15](#).

Figure 2-15 Initialization wizard page of the Moodle dashboard**NOTE**

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
 - The dashboard is being started. Try again later.
2. Locate the resource card and choose **...** > **Reset Password** to reset the password.

For details, see [Resetting the Password for a FlexusL Instance](#).

Figure 2-16 Resetting a password**NOTE**

The password for logging in to the FlexusL instance is also the password for logging in to the O&M page of the application.

Step 4: Initialize Moodle.

Application images use code-based Ubuntu. They provide graphical user interfaces to make your operations easier. You need to initialize the application dashboard upon the first login. Then you can directly log in to the dashboard from the FlexusL console afterwards.

1. In the address bar of a local browser, enter **http://<Server-EIP>:9000** to log in to the application O&M page.

The initial username and password for logging in to the application dashboard are stored on the O&M page of the application. You need to log in to the O&M page first to obtain the username and password. The username for logging in to the O&M page is **root**, and the login password is the one reset in [2](#).

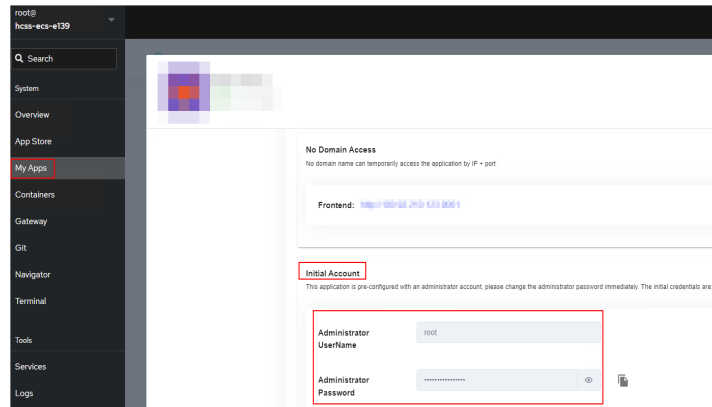
NOTE

For details about the FlexusL instances, O&M page, and dashboard, see [What Is the Relationship Among FlexusL Instances, the Dashboard, and the O&M Page?](#)

2. On the **My Apps** page, click the application icon, choose **Access**, and click **Initial Account** to view the username and password for logging in to the application management page.

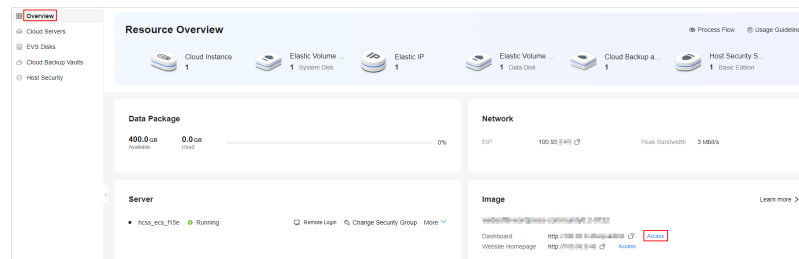
The initial password is a randomly generated strong password. After the application is initialized, change the password on the dashboard for easy

management. If the password is changed, the initial password will be invalid. Remember the new password.



3. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard.

Figure 2-17 Entry to the application dashboard



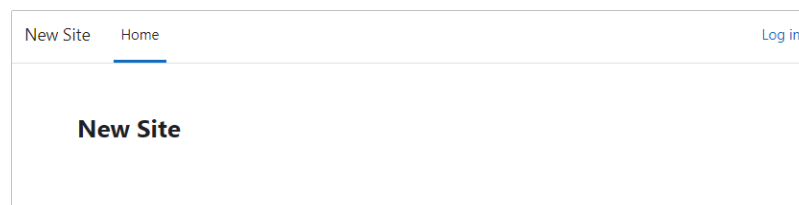
NOTE

If the dashboard is not properly displayed, check the following causes:

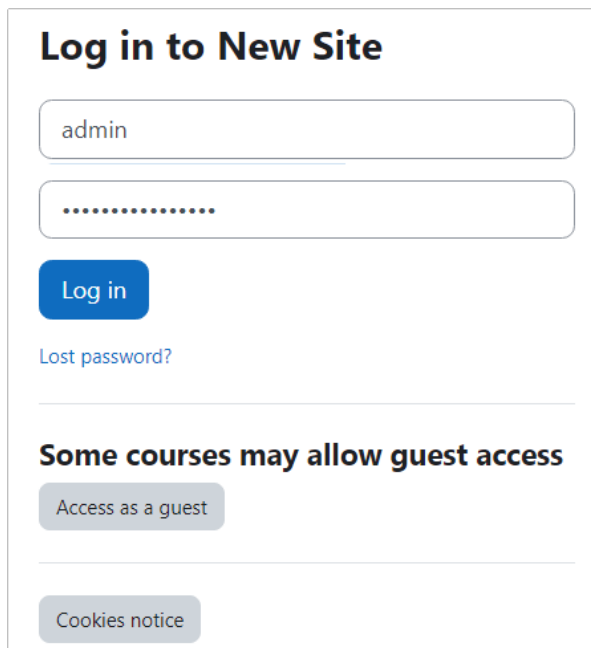
- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
- The dashboard is being started. Try again later.

4. Click **Log in** in the upper right corner.

Figure 2-18 Initialization wizard page of the Moodle dashboard



5. Enter the initial username and password obtained in [2](#) and click **Log in**.



 **NOTE**

If a message is displayed indicating that the username or password you entered is invalid when you attempt to log in to the application dashboard, refer to [Why Can't I Access the Dashboard of the Application Pre-installed in the Application Image After Entering the Initial Username and Password?](#)

After the Moodle application is initialized, you can deploy your applications on the dashboard.

Step 5: Deploy an Application

For details about how to deploy a Moodle application, see [Moodle Service Support](#).

2.6 Using Joomla to Build a Content Management System

Application Scenario

Joomla is a website content management system (CMS) for enterprise websites and e-commerce. It is one of the world's three most popular open source CMSs. The Joomla application image uses the Ubuntu 22.04 and is deployed using Docker. The Joomla application and the required operating environment have been preconfigured. This section describes how to use Joomla to build a CMS.

Resource Planning and Costs

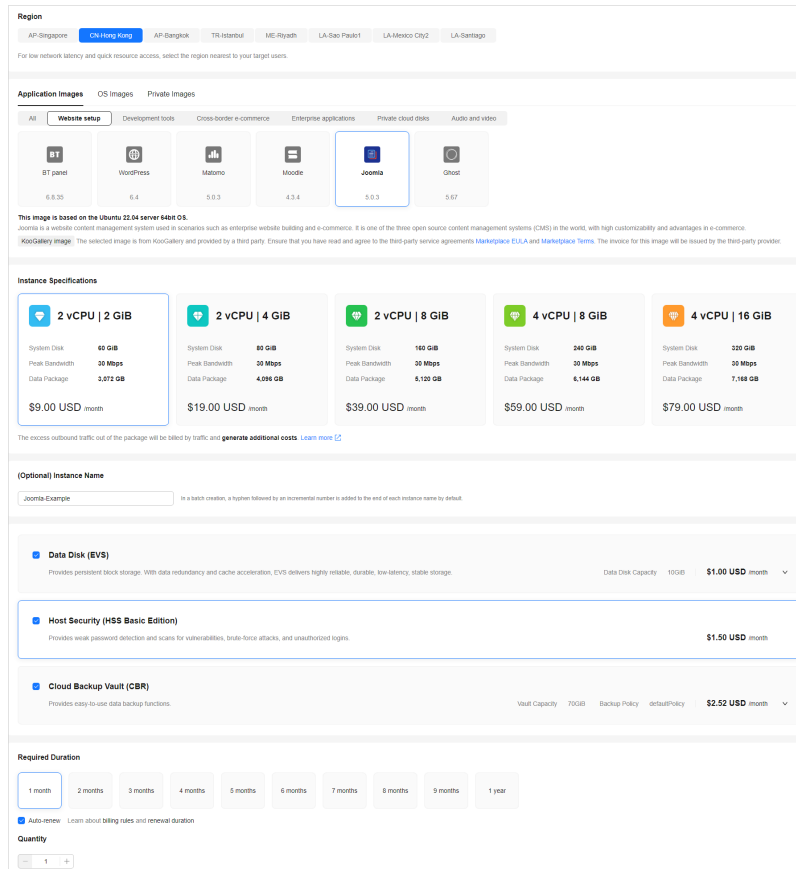
Resource	Configuration	Description
Cloud server	<ul style="list-style-type: none">vCPUs: 2Memory: 2 GiB	In this example, the minimum configuration is selected. You can select the instance specifications based on your service requirements.
Image	Joomla	Select the Joomla application image.
Security group	Inbound rule: <ul style="list-style-type: none">Protocol/ Application: TCPPort: 80, 443, 9000, or 9001Source: 0.0.0.0/0	<ul style="list-style-type: none">80: Specifies the internal forwarding port of an application.443: Allows HTTPS traffic to FlexusL instances.9001: Allows external access to the application dashboard.9000: Allows external access to the application O&M page.

Process

Procedure	Description
Step 1: Purchase FlexusL Instances	Purchase a FlexusL instance and select the Joomla application image.
Step 2: Configure Security Groups	Add inbound security group rules to allow traffic from ports 80, 443, 9000, and 9001 to access the application.
Step 3: Reset a Password	A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance.
Step 4: Initialize Joomla	The image application dashboard needs to be initialized only when you log in for the first time.
Step 5: Build a CMS	This step uses how to install a website template and publish an article as an example to build a CMS with Joomla.

Step 1: Purchase FlexusL Instances

1. Log in to the FlexusL [console](#) and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Application Image	Joomla	Select the Joomla application image.
Instance Specifications	2 vCPUs 2 GiB System disk 60 GiB	Select instance specifications as needed.
Instance Name	Joomla-Example	Customize an instance name that is easy to identify, for example, Joomla-Example.

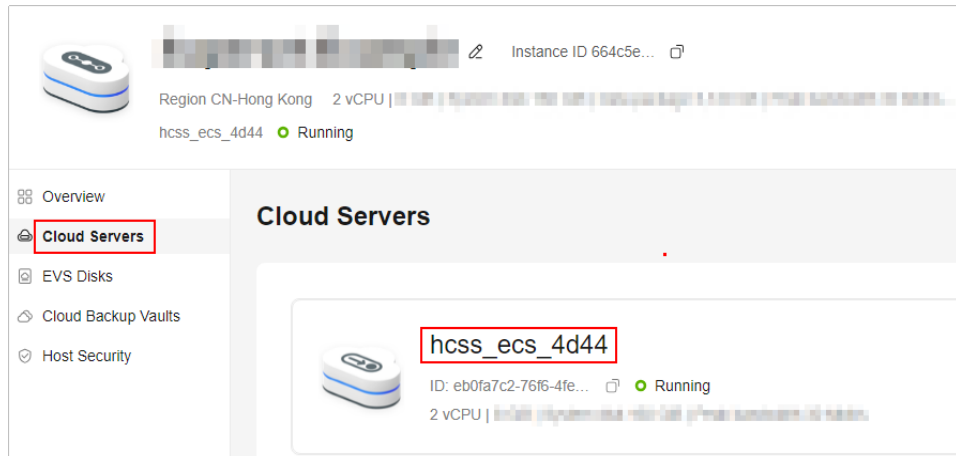
Parameter	Example	Description
(Optional) Associated Service	<ul style="list-style-type: none">• Data Disk: 10 GiB• Host Security• Cloud Backup Vault: 70 GiB	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure Security Groups

Add inbound security group rules to allow traffic from ports 80, 443, 9000, and 9001 to access the application.

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.

The following figure only displays common rules. You can add more rules as needed.

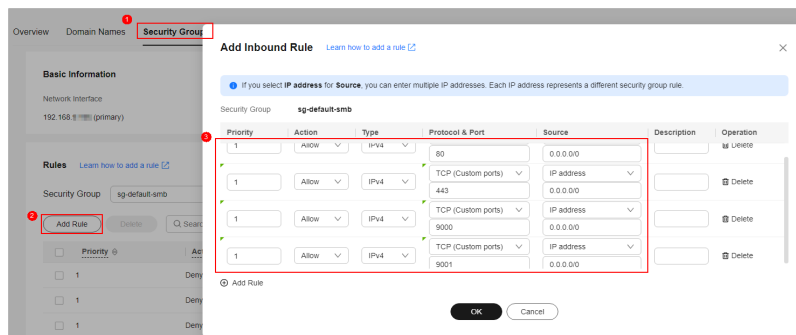


Table 2-7 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of an application.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS traffic to FlexusL instances.
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M page.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

Step 3: Reset a Password

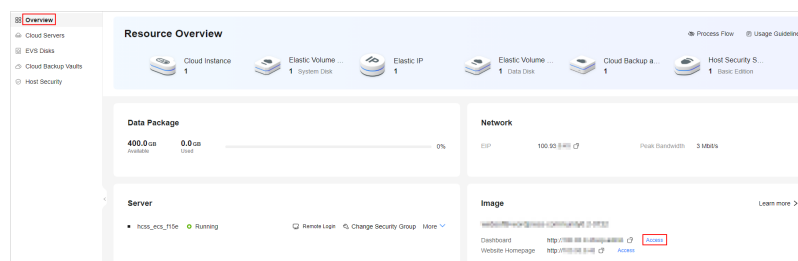
A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance. The password of the FlexusL instance is also used for **logging in to the O&M page of the application**.

1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard and check whether the application has been up and running. If yes, go to the next step.

NOTICE

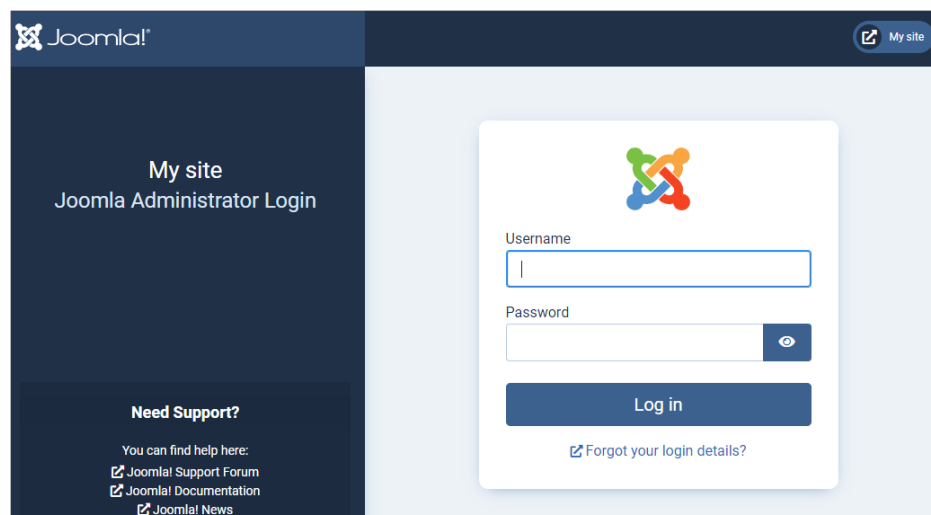
Wait for several minutes until the image with the pre-installed application is up and running. Then, you can perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the initial password may become invalid and you cannot log in to the application dashboard.

Figure 2-19 Entry to the application dashboard



After the application is started, the initialization wizard page of the dashboard is displayed, as shown in **Figure 2-20**.

Figure 2-20 Initialization wizard page of the Joomla dashboard



NOTE

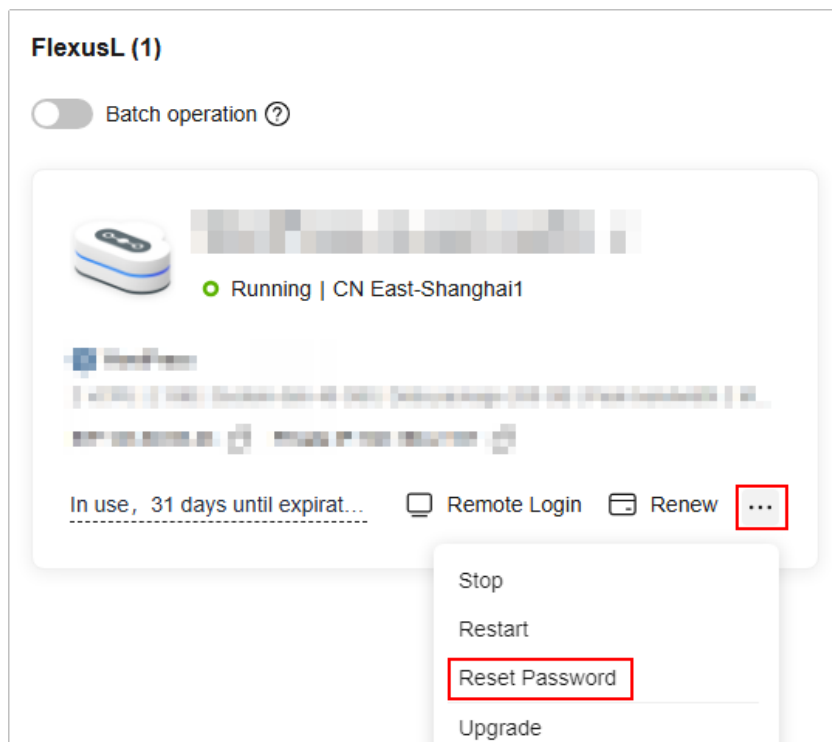
If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on **Step 2: Configure Security Groups**.
- The dashboard is being started. Try again later.

2. Locate the resource card and choose **...** > **Reset Password** to reset the password.

For details, see [Resetting the Password for a FlexusL Instance](#).

Figure 2-21 Resetting a password



NOTE

The password for logging in to the FlexusL instance is also the password for logging in to the O&M page of the application.

Step 4: Initialize Joomla

Application images use code-based Ubuntu. They provide graphical user interfaces to make your operations easier. You need to initialize the application dashboard upon the first login. Then you can directly log in to the dashboard from the FlexusL console afterwards.

1. In the address bar of a local browser, enter **http://<Server-EIP>:9000** to log in to the application O&M page.

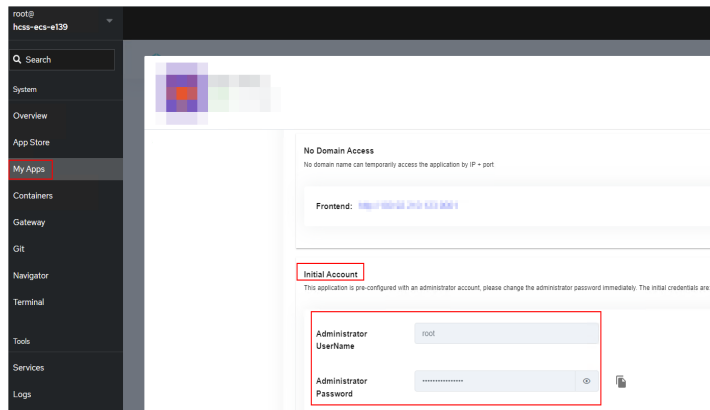
The initial username and password for logging in to the application dashboard are stored on the O&M page of the application. You need to log in to the O&M page first to obtain the username and password. The username for logging in to the O&M page is **root**, and the login password is the password reset in [2](#).

NOTE

For details about the FlexusL instances, O&M page, and dashboard, see [What Is the Relationship Among FlexusL Instances, the Dashboard, and the O&M Page?](#)

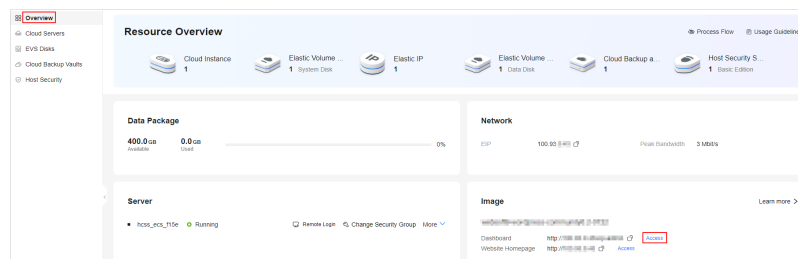
2. On the **My Apps** page, click the application icon, choose **Access**, and click **Initial Account** to view the username and password for logging in to the application management page.

The initial password is a randomly generated strong password. After the application is initialized, change the password on the dashboard for easy management. If the password is changed, the initial password will be invalid. Remember the new password.



3. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard.

Figure 2-22 Entry to the application dashboard

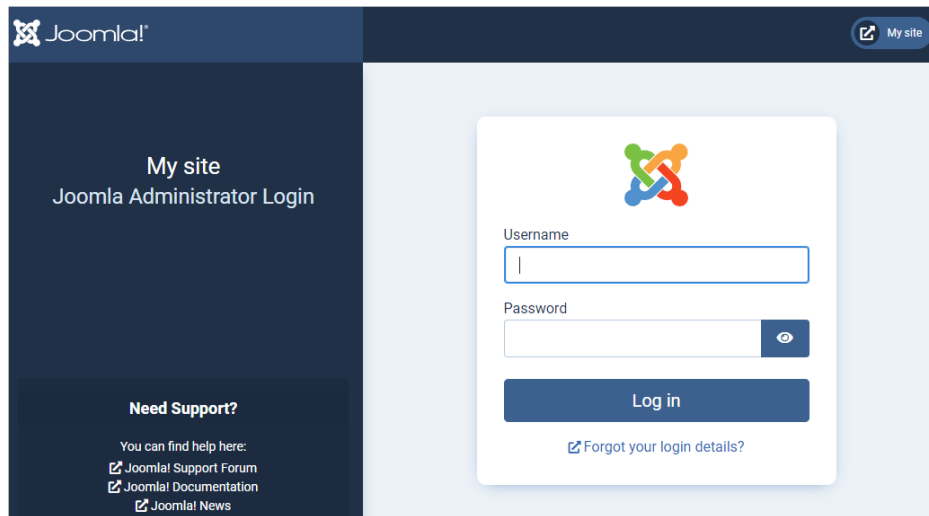


NOTE

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
 - The dashboard is being started. Try again later.
4. Enter the dashboard username and password obtained in [2](#) and click **Log in**.

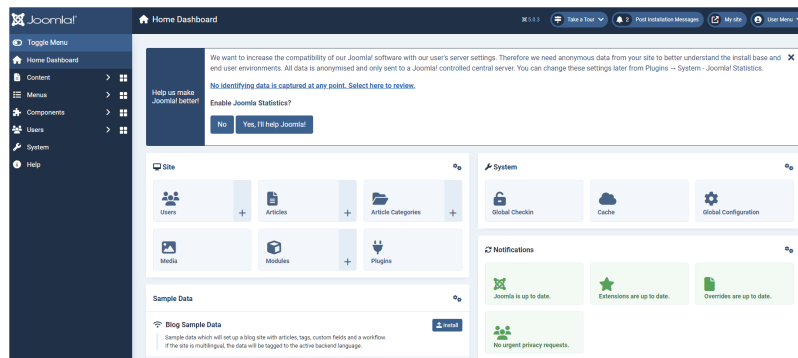
Figure 2-23 Initialization wizard page of the Joomla dashboard



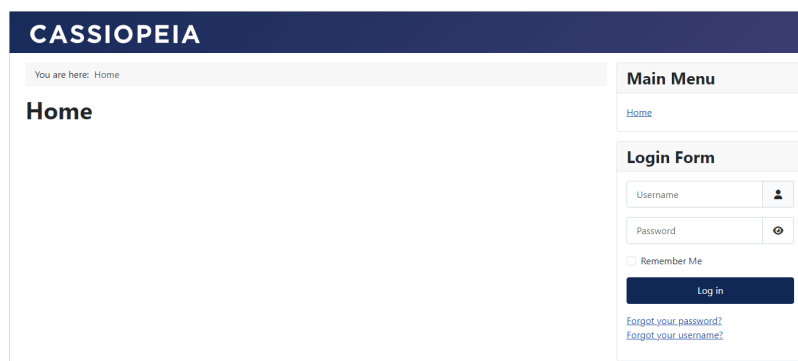
NOTE

If a message is displayed indicating that the username or password you entered is invalid when you attempt to log in to the application dashboard, refer to [Why Can't I Access the Dashboard of the Application Pre-installed in the Application Image After Entering the Initial Username and Password?](#)

5. Check the application dashboard and preview the page of Joomla CMS.
 - After logging in to the dashboard, information similar to the following is displayed.



- Enter `http://<Server-EIP>:9001` in the address bar of the local browser to preview the page of Joomla CMS.
The initialized application page is blank.

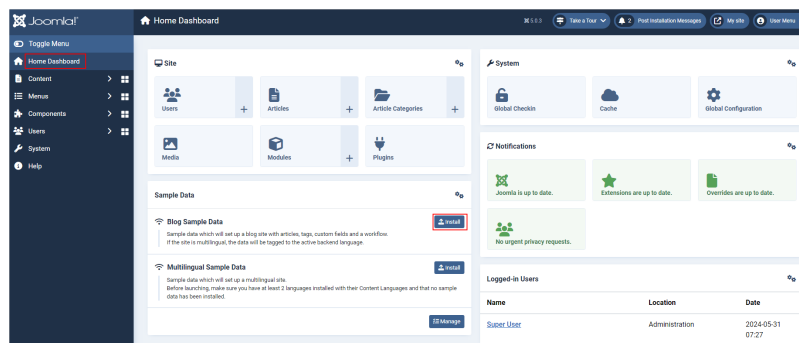


After the Joomla application is initialized, you can deploy your applications on the dashboard.

Step 4: Build a CMS

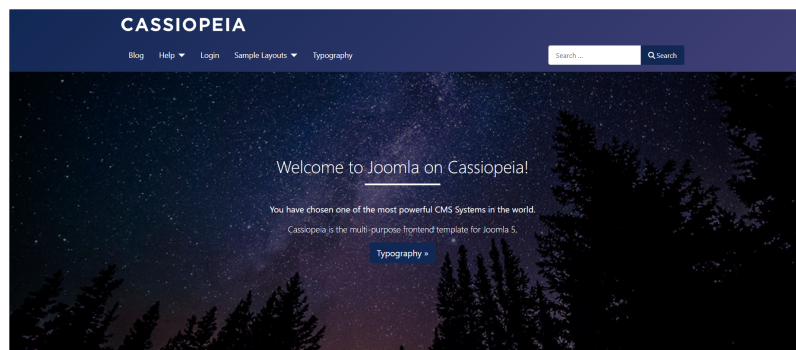
This step uses how to install a website template and publish an article as an example to build a CMS with Joomla.

1. Install a blog template for the website.
 - a. On the default home dashboard of the management page, select **Blog Sample Data** in **Sample Data** and click **Install** to install the blog template.

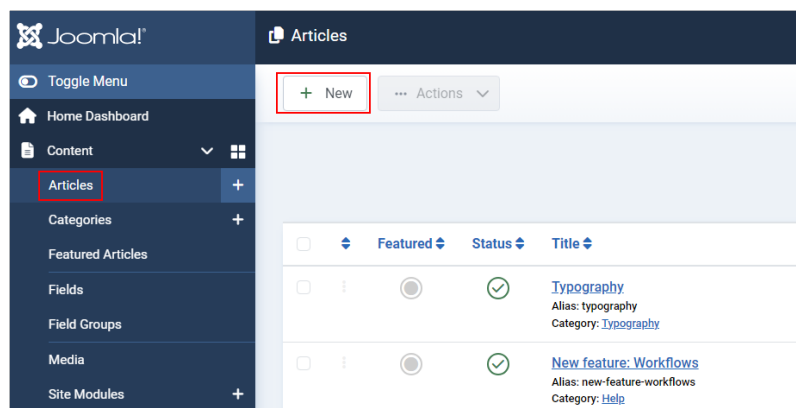


- b. In an address bar of a local browser, enter **http://<Server-EIP>:9001** to access the blog page.

The website content has been templated.

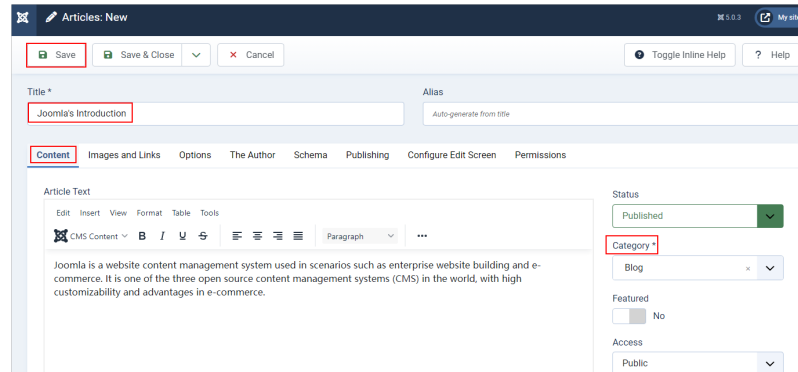


2. Publish an article on the website.
 - a. Choose **Content > Articles** in the navigation pane of the management page and click **New** to create an article.

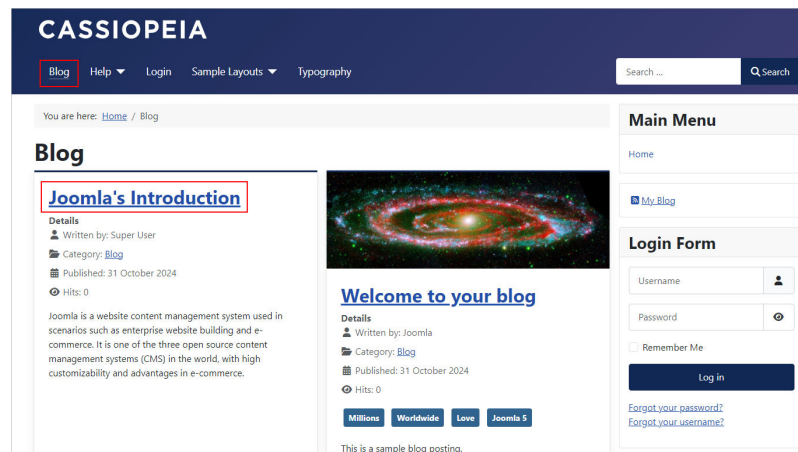


- b. Edit the article title and content in **Title** and **Content**, set the following parameters, and click **Save**.

Categorize articles in **Category**, for example, Blog. You can also set the access permissions and tags of the article.



- c. Click **Blog** on the blog page. Then you can view the article published on the website.



2.7 Using Ghost to Build a Personal Blog

Application Scenario

Ghost is a powerful app for professional publishers to create, share, and grow a business around their content. It comes with modern tools to build a website, publish content, send newsletters, and offer paid subscriptions to members. The Ghost application image uses Ubuntu 22.04 and is deployed using Docker. The Ghost application and the required operating environment have been preconfigured in the Ghost application image. This section describes how to use the Ghost application image to build a personal blog.

Resource Planning and Costs

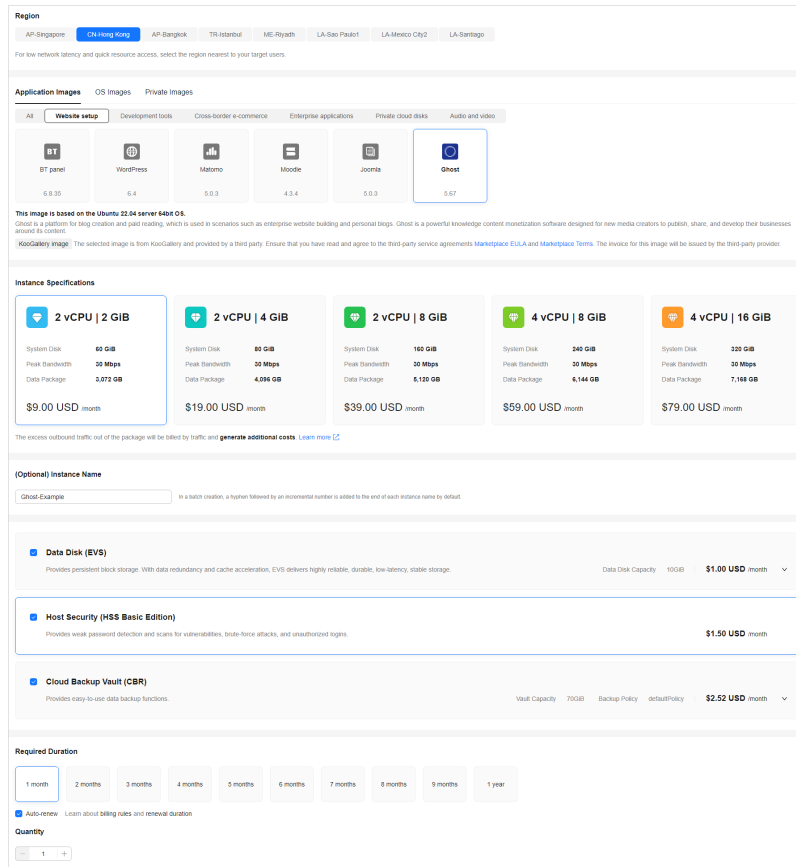
Resource	Configuration	Description
Cloud server	<ul style="list-style-type: none">vCPUs: 2Memory: 2 GiB	Select appropriate instance specifications based on your service requirements.
Image	Ghost	Select the Ghost application image.
Security group	Inbound rule: <ul style="list-style-type: none">Protocol/ Application: TCPPort: 80, 443, 9000, or 9001Source: 0.0.0.0/0	<ul style="list-style-type: none">80: Specifies the internal forwarding port of an application.443: Allows HTTPS traffic to FlexusL instances.9001: Allows external access to the application dashboard.9000: Allows external access to the application O&M page.

Process

Procedure	Description
Step 1: Purchase FlexusL Instances	Purchase a FlexusL instance and select the Ghost application image.
Step 2: Configure Security Groups	Add inbound security group rules to allow traffic from ports 80, 443, 9000, and 9001 to access the application.
Step 3: Reset a Password	A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance.
Step 4: Initialize Ghost	The image application dashboard needs to be initialized only when you log in for the first time.
Step 5: Publish a Post	Use posting as an example to describe how to use the Ghost application image to build a personal blog.

Step 1: Purchase FlexusL Instances

1. Log in to the FlexusL [console](#) and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Application Image	Ghost	Select the Ghost application image.
Instance Specifications	2 vCPUs 2 GiB System disk 60 GiB	Select instance specifications as needed.
Instance Name	Ghost-Example	Customize an instance name that is easy to identify, for example, Ghost-Example.

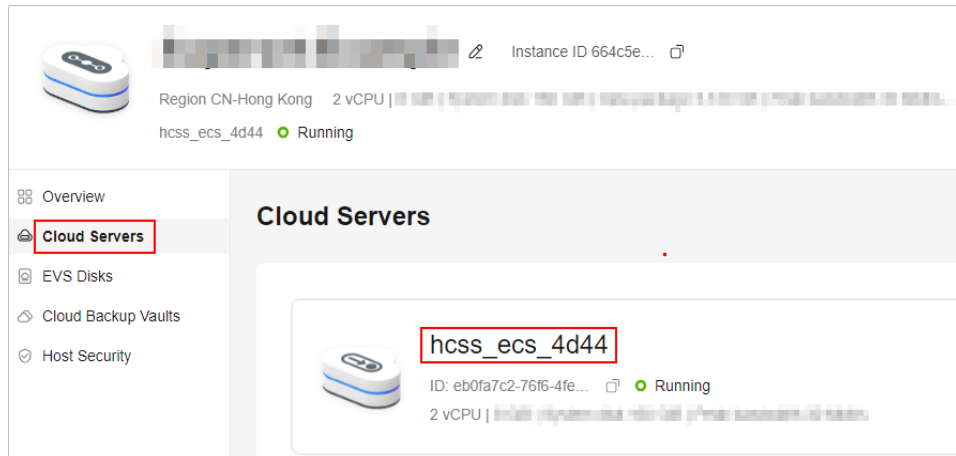
Parameter	Example	Description
(Optional) Associated Service	<ul style="list-style-type: none">• Data Disk: 10 GiB• Host Security• Cloud Backup Vault: 70 GiB	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure Security Groups

Add inbound security group rules to allow traffic from ports 80, 443, 9000, and 9001 to access the application.

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.

The following figure only displays common rules. You can add more rules as needed.

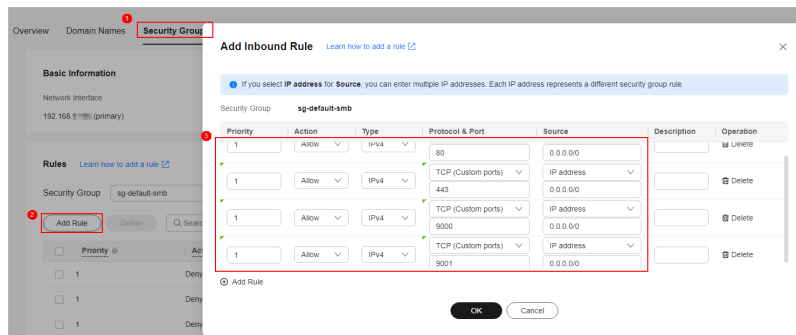


Table 2-8 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of an application.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS traffic to FlexusL instances.
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M page.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

Step 3: Reset a Password

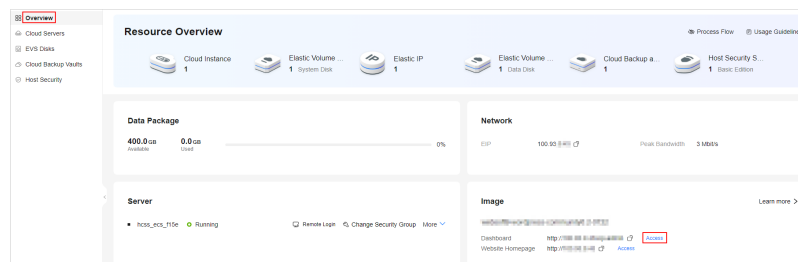
A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance.

1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard and check whether the application has been up and running. If yes, go to the next step.

NOTICE


Wait for several minutes until the image with the pre-installed application is up and running. Then, you can perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the initial password may become invalid and you cannot log in to the application dashboard.

Figure 2-24 Entry to the application dashboard



After the application is started, the initialization wizard page of the dashboard is displayed, as shown in [Figure 2-25](#).

Figure 2-25 Initialization wizard page of the Gost dashboard



Welcome to Ghost.

All over the world, people have started 3,000,000+ incredible sites with Ghost. Today, we're starting yours.

Site title

Full name

Email address

Password

Create account & start publishing →

 **NOTE**

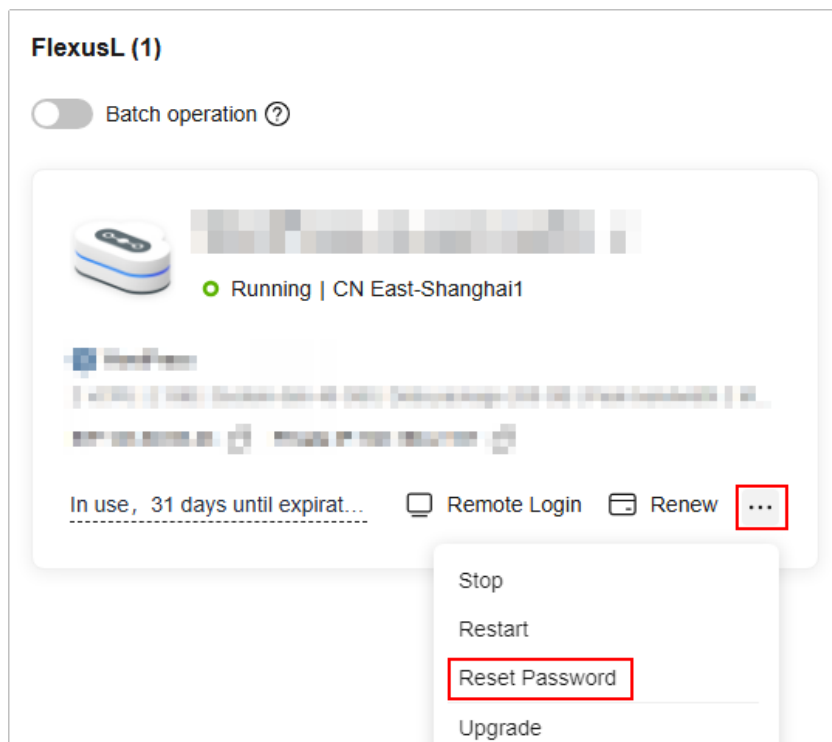
If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
- The dashboard is being started. Try again later.

2. In the resource card, choose  > **Reset Password**, and perform operations as prompted.

For details, see [Resetting the Password for a FlexusL Instance](#).

Figure 2-26 Resetting a password

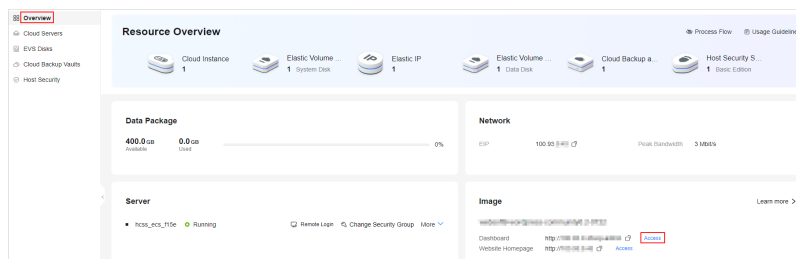


Step 4: Initialize Ghost

Application images use code-based Ubuntu. They provide graphical user interfaces to make your operations easier. You need to initialize the application dashboard upon the first login. Then you can directly log in to the dashboard from the FlexusL console afterwards.

1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard.

Figure 2-27 Entry to the application dashboard

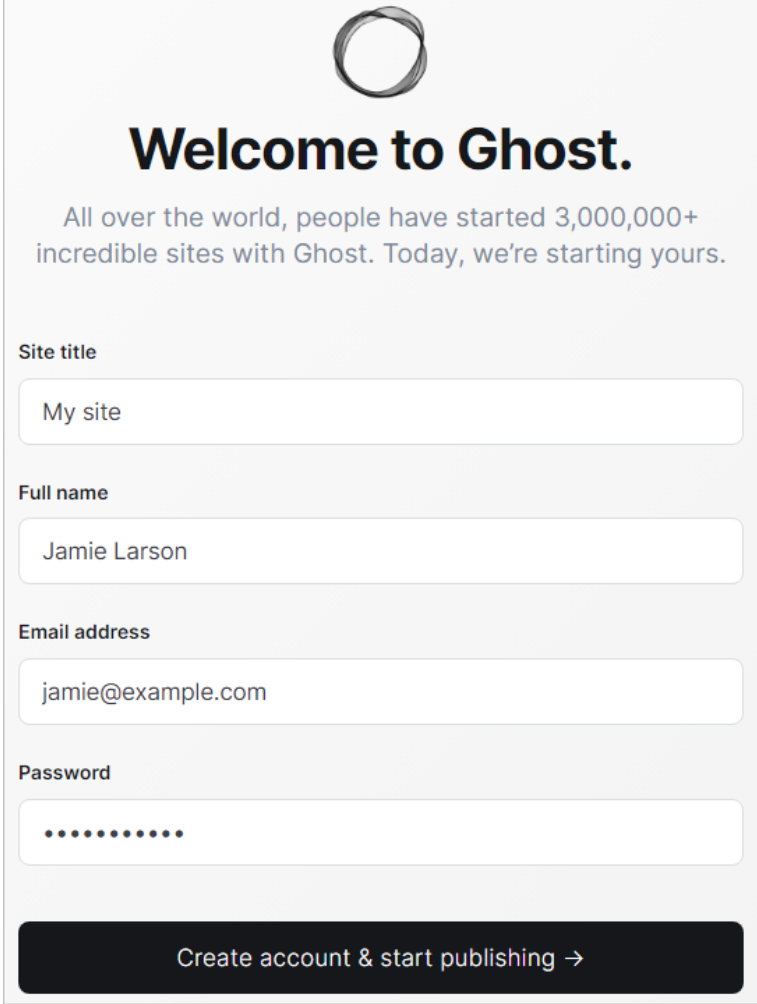


NOTE

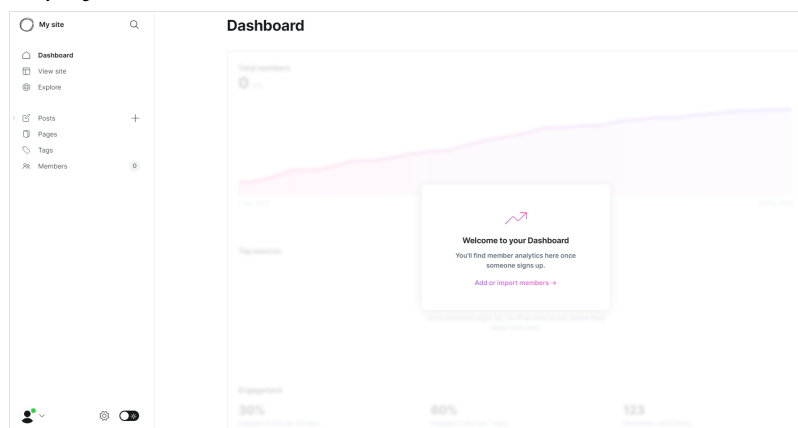
- If the dashboard is not properly displayed, check the following causes:
- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
 - The dashboard is being started. Try again later.
2. Set the website title, username, email address, and password, and click **Create account & start publishing** to create an account and deploy the application.

The email address and password are credentials for logging in to the dashboard.

Figure 2-28 Initialization wizard page of the Gost dashboard

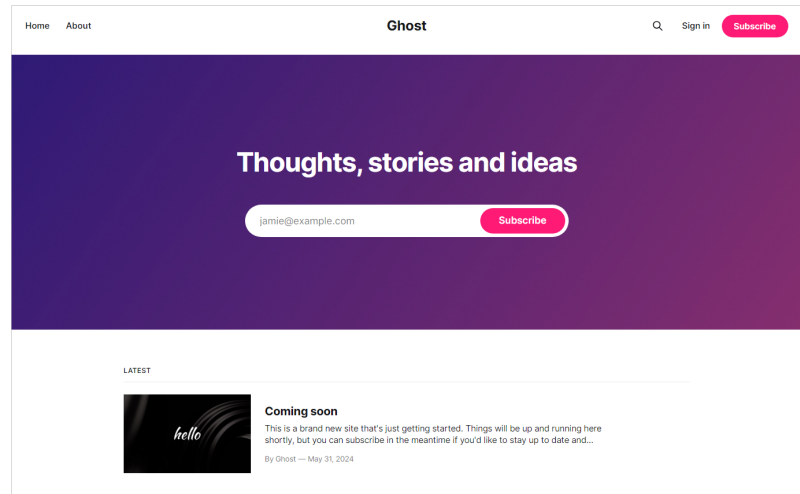


3. Check the dashboard and web portal of the application.
 - After logging in to the dashboard, information similar to the following is displayed.



- In an address box of a local browser, enter **http://<Server-EIP>:9001** to access the web portal.

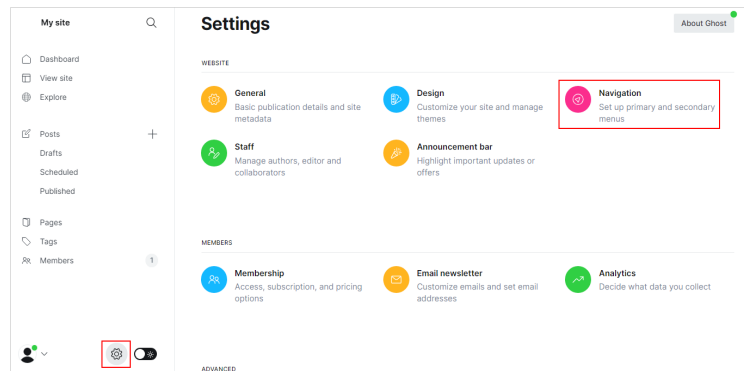
If you have added a domain name, you can also use **http://<wpwebsite.com>:9001** to access the web portal.



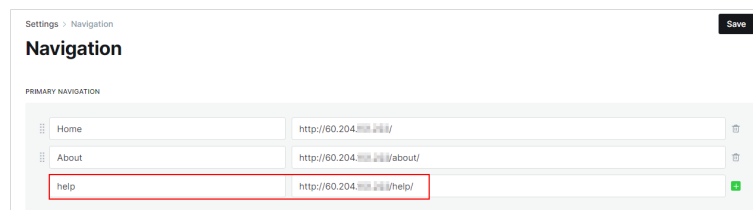
After the Ghost application is initialized, you can publish your posts on the dashboard.

Step 5: Publish a Post

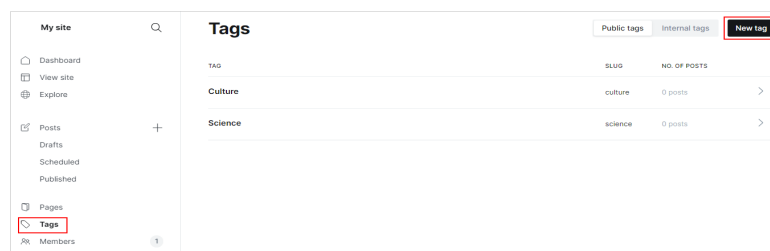
1. On the dashboard, click the setting icon and click **Navigation** to add a menu.



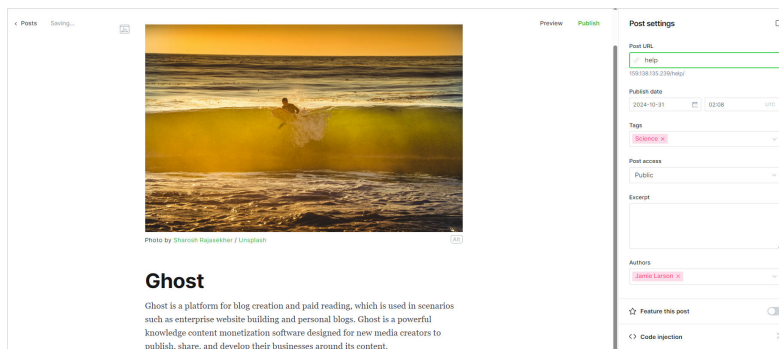
2. Edit the menu name and URL and click **Save**.



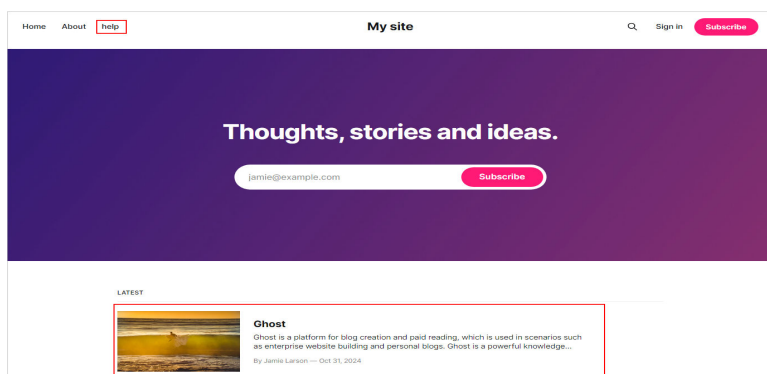
3. Select **Tags** and click **New tag** to set a tag type for the blog post.



4. Choose **Posts**, click **New post** in the upper right corner, and click **Publish**.
After editing the image, title, and content for a post, you can add tags to the post for classification.



5. In an address bar of a local browser, enter **http://<Server-IP>:9001** to view the created **help** menu and released documents.



2.8 Using EspoCRM to Build a Content Management System

Application Scenario

EspoCRM an open source customer relationship management (CRM) platform accessible on PCs, mobile phones, and tablets. It provides functions including sales automation, marketing, sales process, documentations, products, contracts, knowledge base, and workflow. The EspoCRM application image uses the Ubuntu 22.04 and is deployed using Docker. The EspoCRM application and the required operating environment have been preconfigured. This section describes how to use EspoCRM to build a CMS.

Resource Planning and Costs

Resource	Configuration	Description
Cloud server	<ul style="list-style-type: none"> vCPUs: 2 Memory: 2 GiB 	Select appropriate instance specifications based on your service requirements.

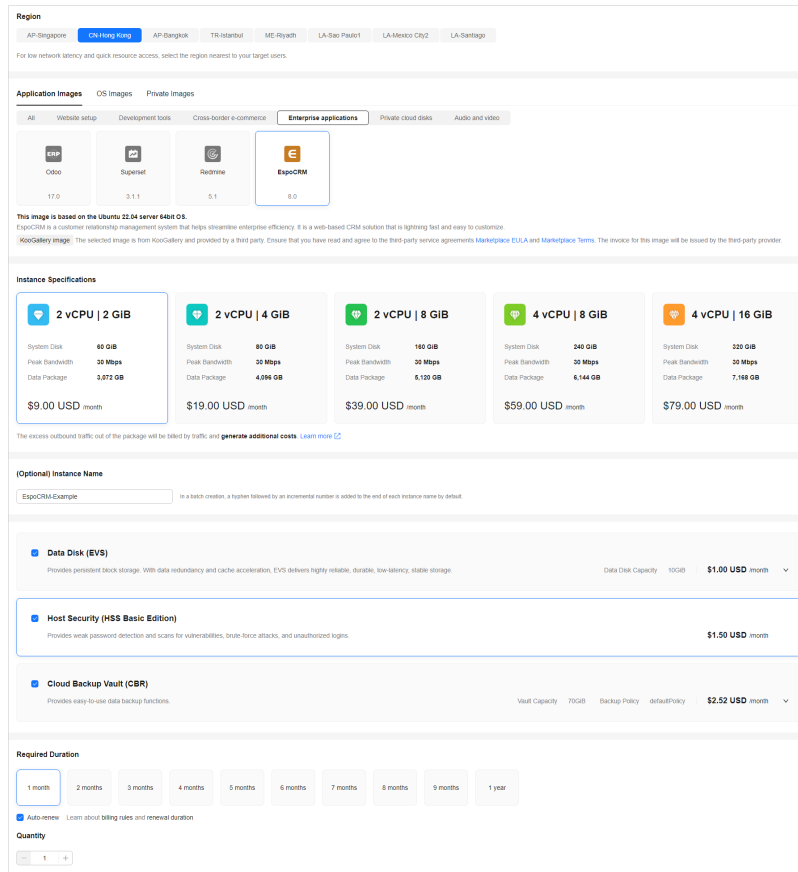
Resource	Configuration	Description
Image	EspoCRM	Select the EspoCRM application image.
Security group	Inbound rule: <ul style="list-style-type: none">• Protocol/ Application: TCP• Port: 80, 443, 9000, or 9001• Source: 0.0.0.0/0	<ul style="list-style-type: none">• 80: Specifies the internal forwarding port of an application.• 443: Allows HTTPS traffic to FlexusL instances.• 9001: Allows external access to the application dashboard.• 9000: Allows external access to the application O&M page.

Process

Procedure	Description
Step 1: Purchase FlexusL Instances	Purchase a FlexusL instance and select the EspoCRM application image.
Step 2: Configure Security Groups	Add inbound security group rules to allow traffic from ports 80, 443, 9000, and 9001 to access the application.
Step 3: Reset a Password	A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance.
Step 4: Initialize EspoCRM	The image application dashboard needs to be initialized only when you log in for the first time.

Step 1: Purchase FlexusL Instances

1. Log in to the FlexusL [console](#) and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Application Image	EspoCRM	Select the EspoCRM application image.
Instance Specifications	2 vCPUs 2 GiB System disk 60 GiB	Select instance specifications as needed.
Instance Name	EspoCRM-Example	Customize an instance name that is easy to identify, for example, EspoCRM-Example.

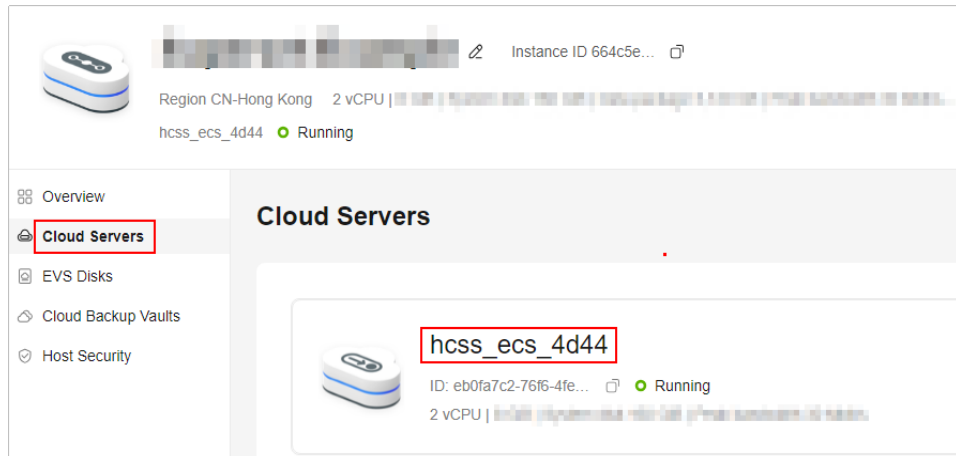
Parameter	Example	Description
(Optional) Associated Service	<ul style="list-style-type: none">• Data Disk: 10 GiB• Host Security• Cloud Backup Vault: 70 GiB	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure Security Groups

Add inbound security group rules to allow traffic from ports 80, 443, 9000, and 9001 to access the application.

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.

The following figure only displays common rules. You can add more rules as needed.

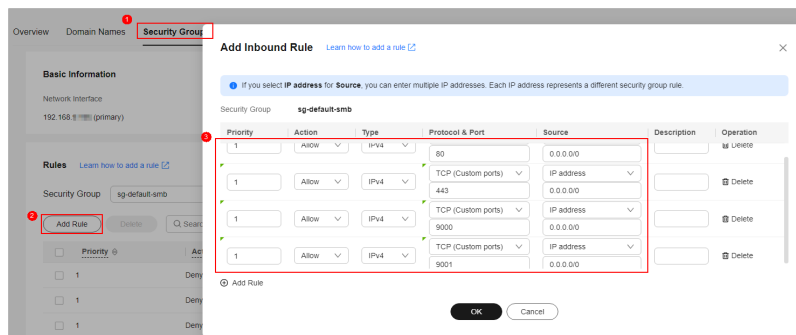


Table 2-9 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of an application.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS traffic to FlexusL instances.
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M page.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

Step 3: Reset a Password

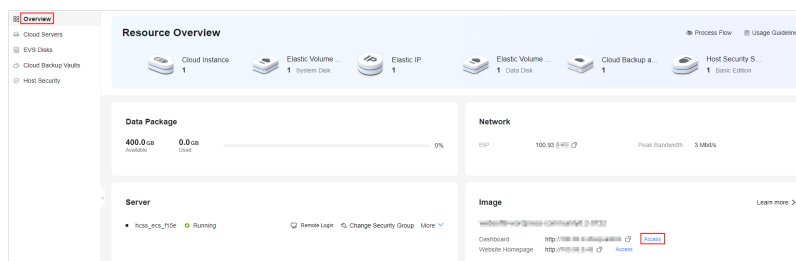
A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance. The password of the FlexusL instance is also used for **logging in to the O&M page of the application**.

1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard and check whether the application has been up and running. If yes, go to the next step.

NOTICE

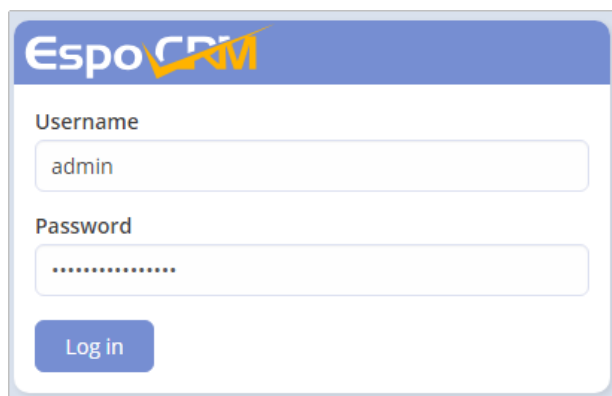
Wait for several minutes until the image with the pre-installed application is up and running. Then, you can perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the initial password may become invalid and you cannot log in to the application dashboard.

Figure 2-29 Entry to the application dashboard



After the application is started, the initialization wizard page of the dashboard is displayed, as shown in [Figure 2-30](#).

Figure 2-30 Initialization wizard page of the EspoCRM dashboard



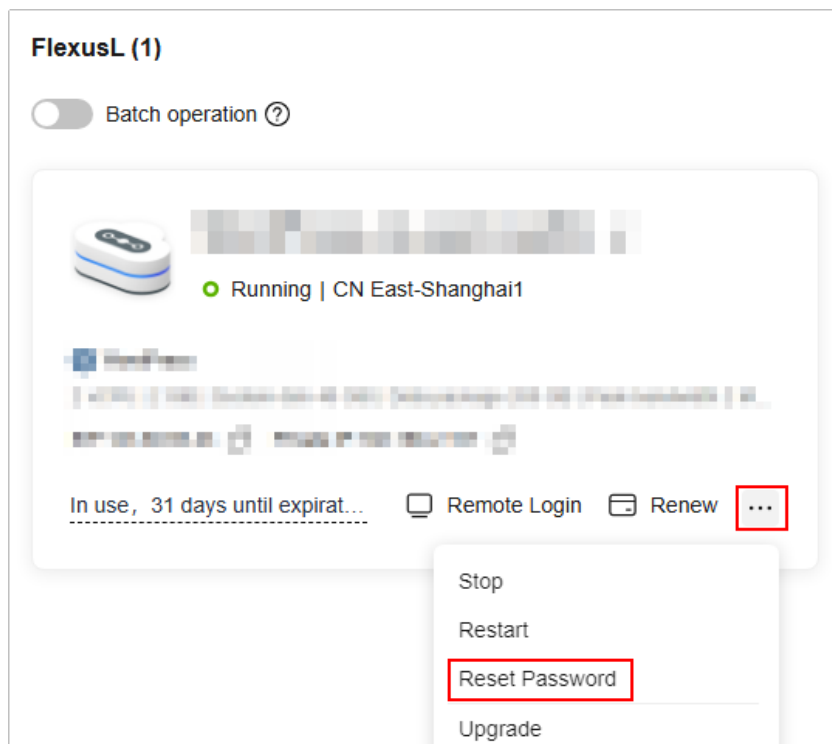
NOTE

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
 - The dashboard is being started. Try again later.
2. Locate the resource card and choose **...** > **Reset Password** to reset the password.

For details, see [Resetting the Password for a FlexusL Instance](#).

Figure 2-31 Resetting a password

**NOTE**

The password for logging in to the FlexusL instance is also the password for logging in to the O&M page of the application.

Step 4: Initialize EspoCRM

Application images use code-based Ubuntu. They provide graphical user interfaces to make your operations easier. You need to initialize the application dashboard upon the first login. Then you can directly log in to the dashboard from the FlexusL console afterwards.

1. In the address bar of a local browser, enter **http://<Server-EIP>:9000** to log in to the application O&M page.

The initial username and password for logging in to the application dashboard are stored on the O&M page of the application. You need to log in to the O&M page first to obtain the username and password. The username for logging in to the O&M page is **root**, and the login password is the password reset in [2](#).

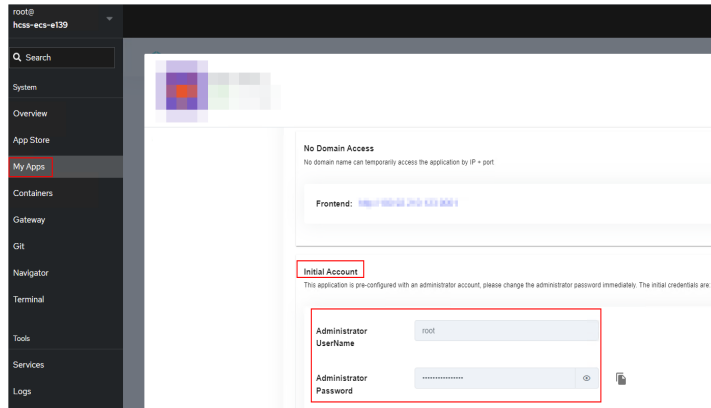
NOTE

For details about the FlexusL instances, O&M page, and dashboard, see [What Is the Relationship Among FlexusL Instances, the Dashboard, and the O&M Page?](#)

2. On the **My Apps** page, click the application icon, choose **Access**, and click **Initial Account** to view the username and password for logging in to the application management page.

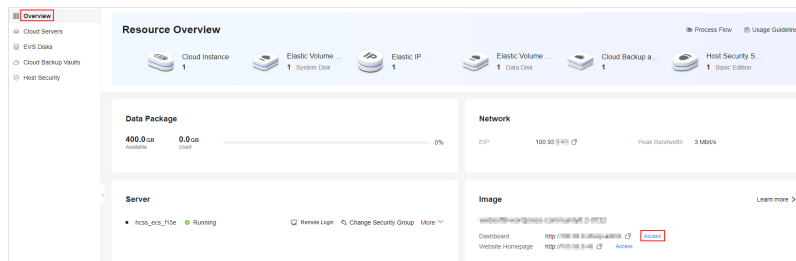
The initial password is a randomly generated strong password. After the application is initialized, change the password on the dashboard for easy

management. If the password is changed, the initial password will be invalid. Remember the new password.



3. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard.

Figure 2-32 Entry to the application dashboard

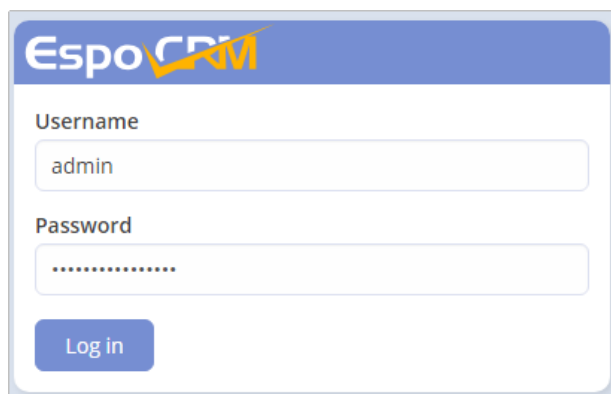


NOTE

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
 - The dashboard is being started. Try again later.
4. On the displayed login page, enter the initial username and password obtained in 2 and click **Log in**.

Figure 2-33 Initialization wizard page of the EspoCRM dashboard

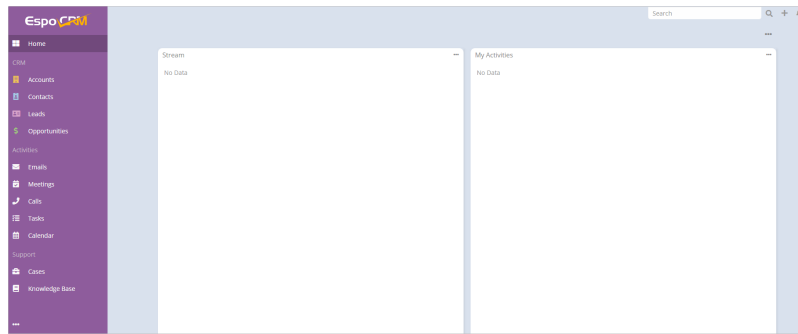


 **NOTE**

If a message is displayed indicating that the username or password you entered is invalid when you attempt to log in to the application dashboard, refer to [Why Can't I Access the Dashboard of the Application Pre-installed in the Application Image After Entering the Initial Username and Password?](#)

5. Check the application dashboard.

After logging in to the application management page, information similar to the following is displayed.



After the EspoCRM application is initialized, you can deploy your applications on the dashboard.

3 Setting Up the Development Environment

3.1 Using Portainer to Deploy a MySQL Container

Application Scenario

Portainer is a graphical tool for Docker management. It offers a range of functions such as status display, quick deployment of application templates, basic operations on Docker (containers, images, networks, and database logical volumes), log display, container console operations, centralized management and operations of Swarm clusters and services, and user login management and control. Supported By FlexusL, the Portainer application image uses Ubuntu 22.04 and is deployed using Docker. The Docker and Portainer have been preconfigured in the image. You can use this application image to visualize Docker management.

Resource Planning and Costs

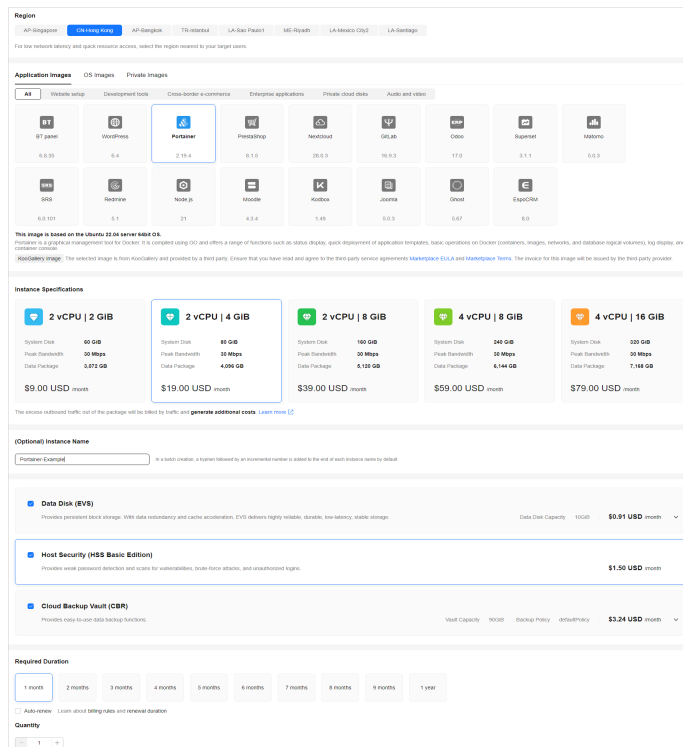
Resource	Configuration	Description
Cloud server	<ul style="list-style-type: none">vCPUs: 2Memory: 4 GiB	Select appropriate instance specifications based on your service requirements.
Image	Portainer	Select the Portainer application image.
Security group	Inbound rule: <ul style="list-style-type: none">Protocol/ Application: TCPPort: 80,9001,3306Source: 0.0.0.0/0	<ul style="list-style-type: none">3306: Allows access to MySQL databases.80: Specifies the internal forwarding port of application images.9000: Allows external access to the application O&M page.9001: Allows external access to the application dashboard.

Process

Procedure	Description
Step 1: Purchase a FlexusL Instance	Purchase a FlexusL instance and select the Portainer application image.
Step 2: Configure Security Groups	Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.
Step 3: Reset the Password and Log In to the FlexusL Instance	A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance before logging in to it.
Step 4: Initialize Portainer	Log in to the dashboard and install and initialize Portainer.
Step 5: Use Portainer to Deploy a MySQL Container	Use Portainer to visualize Docker management (using MySQL container as an example)

Step 1: Purchase a FlexusL Instance

1. Log in to the FlexusL [console](#) and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



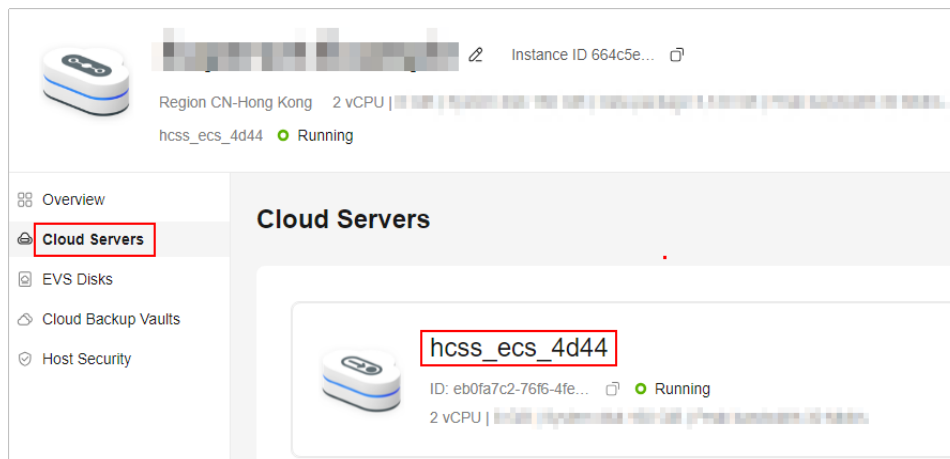
Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Application Image	Portainer	Select the Portainer application image.
Instance Specifications	2 vCPUs 4 GiB memory and 80 GiB system disk	Select instance specifications as needed.
Instance Name	Portainer-Example	Customize an instance name that is easy to identify, for example, Portainer-Example.
(Optional) Associated Services	<ul style="list-style-type: none">• Data disk: 10 GiB• Host security• Cloud backup vault: 90 GiB	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure Security Groups

Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.

The following figure only displays common rules. You can add more rules as needed.

Table 3-1 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of application images
1	Allow	IPv4	TCP: 3306	0.0.0.0/0	Allows access to MySQL databases.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

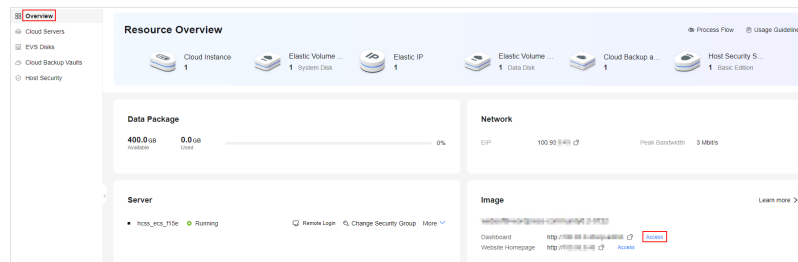
Step 3: Reset the Password and Log In to the FlexusL Instance

This section describes how to log in to a FlexusL instance. A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance before logging in to it.

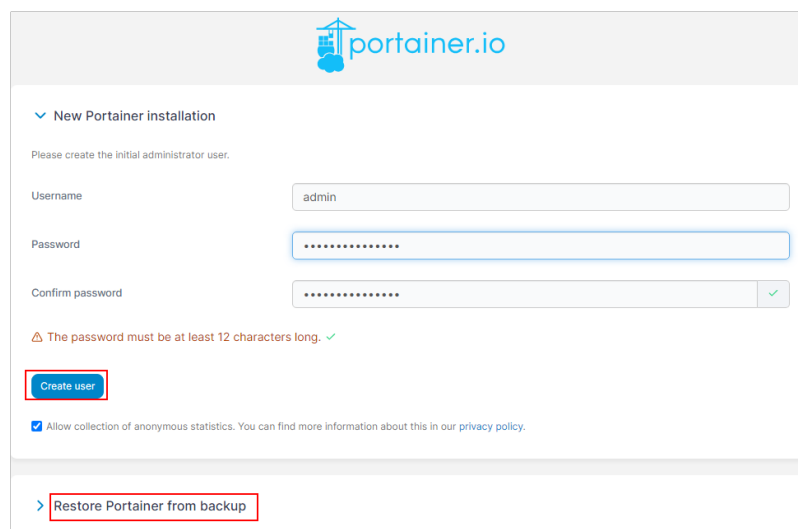
1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard and check whether the application has been up and running. If yes, go to the next step.

NOTICE

Wait for several minutes until the image with the pre-installed application is up and running. Then, you can perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the initial password may become invalid and you cannot log in to the application dashboard.

Figure 3-1 Entry to the application dashboard

After the application is started, the initialization wizard page of the dashboard is displayed, as shown in [Figure 3-2](#).

Figure 3-2 Initialization wizard page of the Portainer dashboard

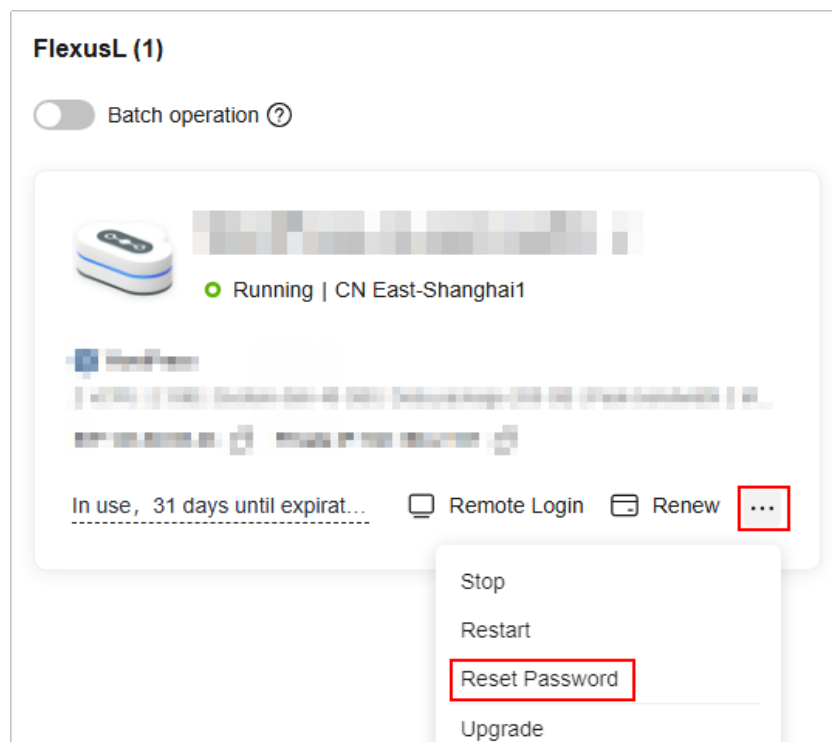
NOTE

If the dashboard is not properly displayed, check the following causes:

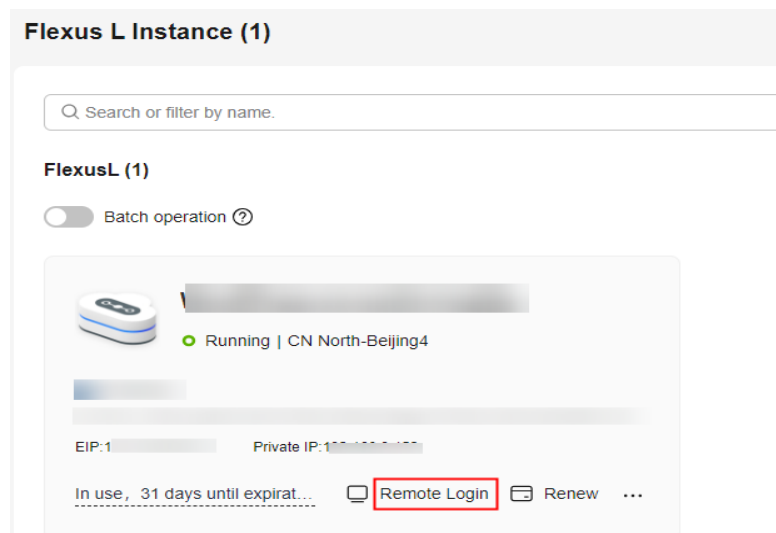
- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
 - The dashboard is being started. Try again later.
2. Locate the resource card and choose **...** > **Reset Password** to reset the password.

A FlexusL instance does not have an initial password. Set a password for the FlexusL instance before logging in to it. For details, see [Resetting the Password for a FlexusL Instance](#).

Figure 3-3 Resetting a password



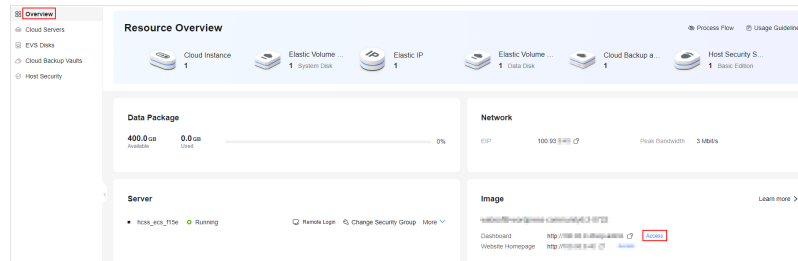
3. Locate the target instance and click **Remote Login** and enter the username and password as prompted to log in to the FlexusL instance. The username is **root**, and the password is the one set in 2.



Step 4: Initialize Portainer

Application images use code-based Ubuntu. They provide graphical user interfaces to make your operations easier. You need to initialize the application dashboard upon the first login. Then you can directly log in to the dashboard from the FlexusL console afterwards.

1. On the **Overview** page, click **Access** in the **Dashboard** field in the **Image** area.

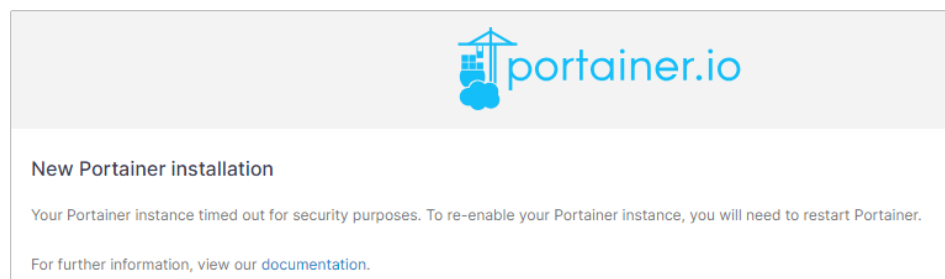


NOTE

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
- The dashboard is being started. Try again later.

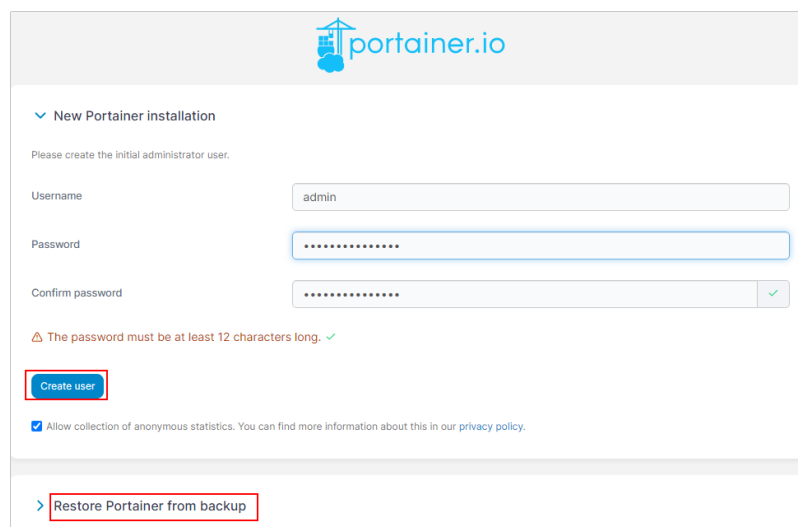
If you use a Portainer application image to create, reinstall, or change the OS of a FlexusL instance, Portainer initialization has a certain validity period. If no users are created within the validity period, a message in the following figure is displayed. In this case, [log in to the server](#) and run `sudo docker restart portainer` to restart Portainer, and then create a user as soon as possible.



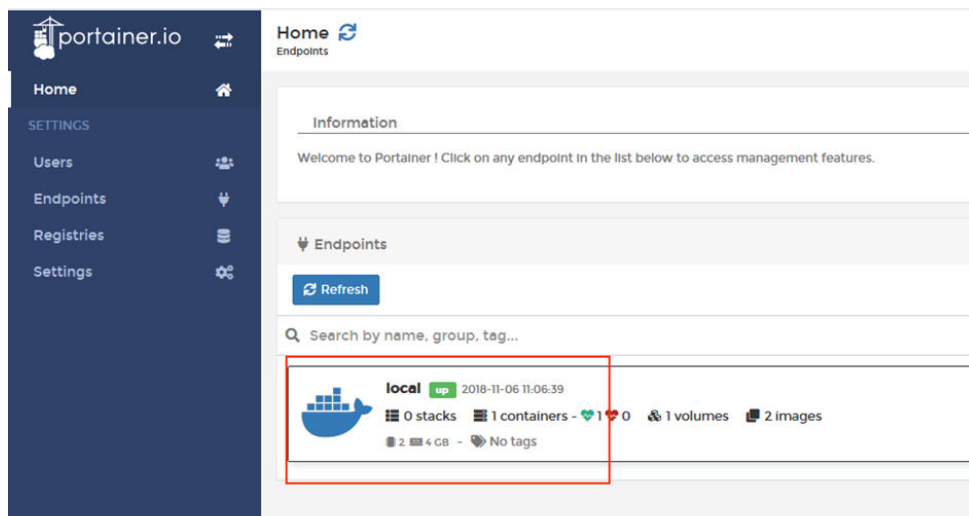
2. Set the username and password of the Portainer administrator and click **Create user**.

If you have backup data for Portainer, click **Restore Portainer from backup** and upload the backup data to quickly set up the Portainer environment.

Figure 3-4 Initialization wizard page of the Portainer dashboard



3. Choose **Home** and click **local** to use Portainer for Docker visual management.



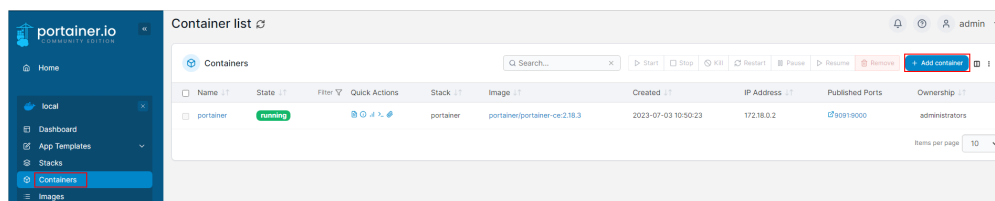
After the Portainer application is initialized, you can deploy your containers on the dashboard.

Step 5: Use Portainer to Deploy a MySQL Container

This section uses the MySQL container as an example to describe how to use Portainer to visualize Docker management.

Step 1: Create a MySQL Container

1. Choose **Containers** in the left navigation pane and click **Add container**.

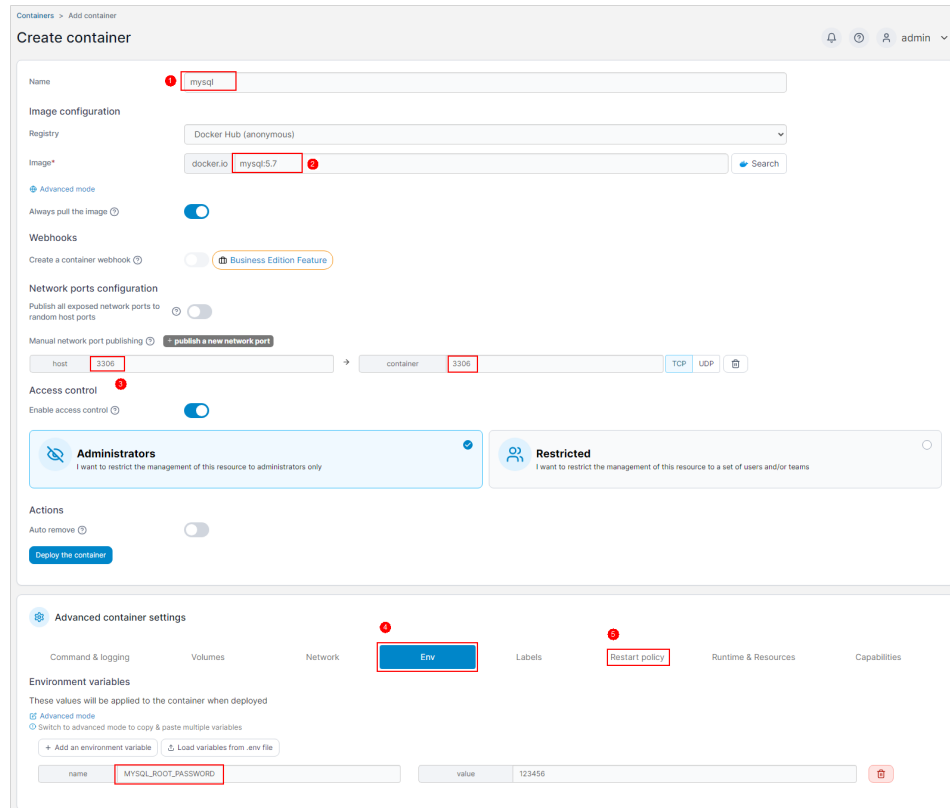


2. Specify MySQL container parameters.
 - ① **Name**: user-defined container name.
 - ② **Image**: container image name. For example, if you set this parameter to **mysql:5.7**, the system automatically pulls the MySQL5.7 container image from Docker Hub.
 - ③ Click **publish a new network port** and add port 3306 to ensure that the MySQL database can be accessed.
 - ④ **Env**: environment variables.
 - **MYSQL_ROOT_PASSWORD**: password of the root user of the database. This parameter is mandatory. It is used for logging in to the MySQL container. Keep the password secure.

NOTE


Ensure that the **MYSQL_ROOT_PASSWORD** parameter name is correctly entered, or the database cannot be connected.

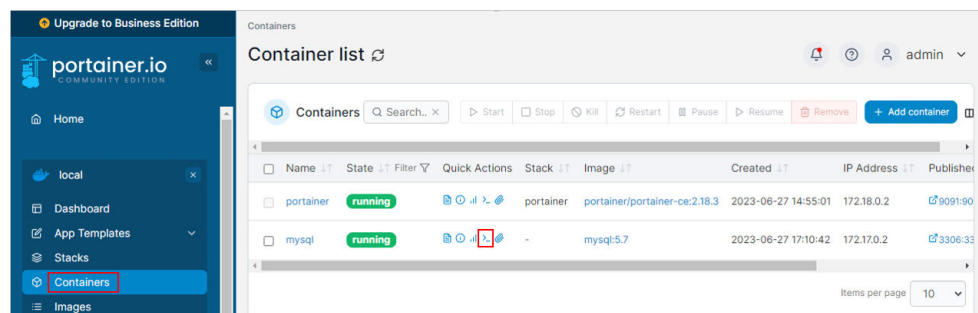
- **MYSQL_DATABASE:** name (such as *wordpress*) of the database which is automatically created in the **value** row after the MySQL container is created. This parameter is optional.
- ⑤ **Restart policy:** You are advised to select **Always** so that the container is always automatically restarted when it is stopped.



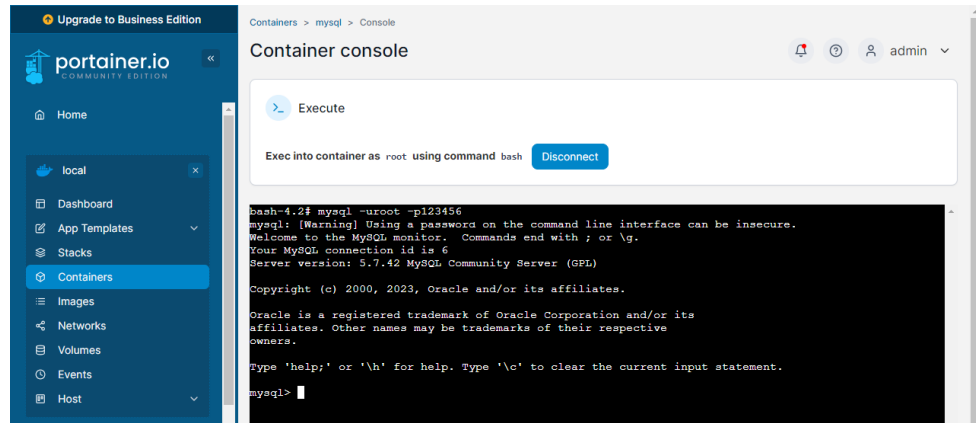
3. Click **Deploy the container** to create a MySQL container.

Step 2: Connect to the MySQL Container

1. Return to the container list and click  in the MySQL container row.



2. On the displayed page, click **Connect** to connect to the container.
3. Run the following command to log in to the MySQL database:
mysql -uroot -p123456, in which **123456** is the value of **MYSQL_ROOT_PASSWORD**.



3.2 Using Node.js to Run Node.js Programs

Application Scenario

Node.js is an open-source project management software. It provides functions such as project management, Wiki, and news, and integrates tools such as GIT, SVN, and CVS. The Node.js application image uses Ubuntu 22.04 and is deployed using Docker. The Node.js application and the required operating environment have been preconfigured in the Node.js application image. This section describes how to use a Node.js application image to run a Node.js application.

Resource Planning and Costs

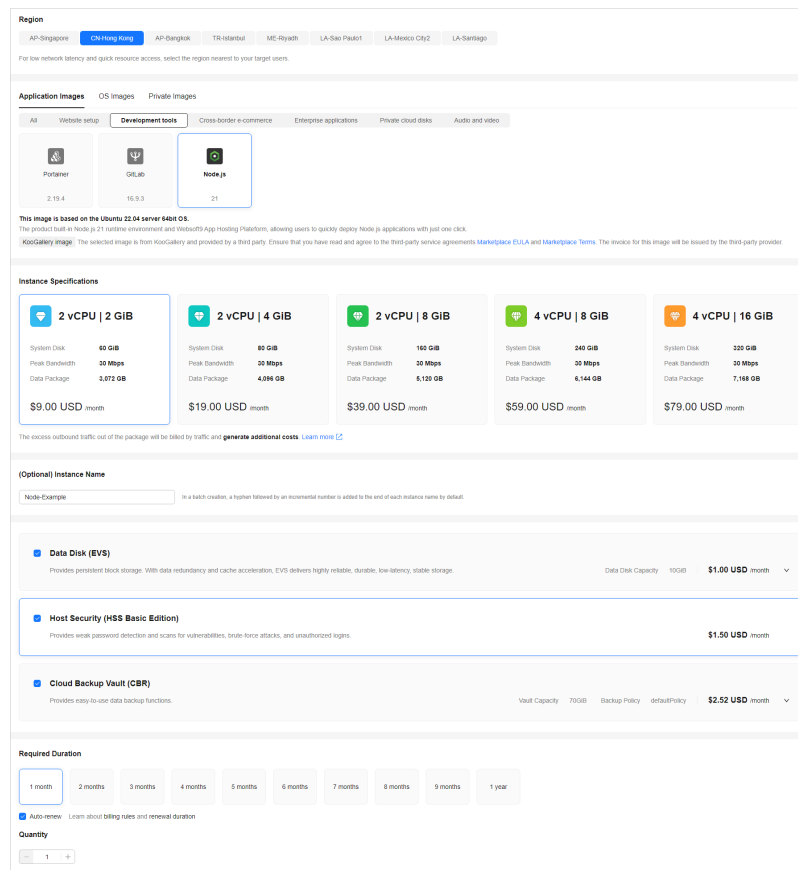
Resource	Configuration	Description
Cloud server	<ul style="list-style-type: none"> vCPUs: 2 Memory: 2 GiB 	Select appropriate instance specifications based on your service requirements.
Image	Node.js	Select the Node.js application image.
Security group	Inbound rule: <ul style="list-style-type: none"> Protocol/ Application: TCP Port: 80, 443, 9000, or 9001 Source: 0.0.0.0/0 	<ul style="list-style-type: none"> 80: Specifies the internal forwarding port of an application. 443: Allows HTTPS traffic to FlexusL instances. 9001: Allows external access to the application dashboard. 9000: Allows external access to the application O&M page.

Process

Procedure	Description
Step 1: Purchase FlexusL Instances	Purchase a FlexusL instance and select the Node.js application image.
Step 2: Configure Security Groups	Add inbound security group rules to allow traffic from ports 80, 443, 9000, and 9001 to access the application.
Step 3: Run the Node.js Program	Use the Node.js application image to run a Node.js application.

Step 1: Purchase FlexusL Instances

1. Log in to the FlexusL [console](#) and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



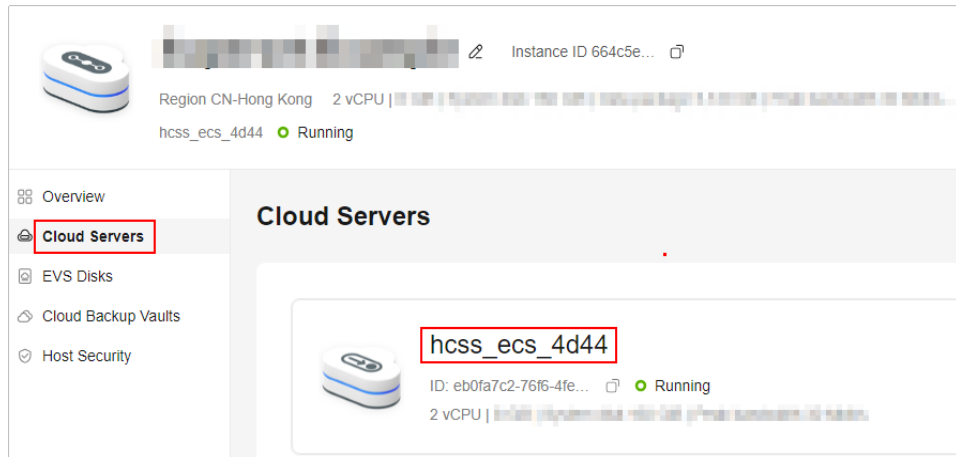
Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Application Image	Node.js	Select the Node.js application image.
Instance Specifications	2 vCPUs 2 GiB System disk 60 GiB	Select instance specifications as needed.
Instance Name	Node-Example	Customize an instance name that is easy to identify, for example, Node-Example.
(Optional) Associated Service	<ul style="list-style-type: none">• Data Disk: 10 GiB• Host Security• Cloud Backup Vault: 70 GiB	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure Security Groups

Add inbound security group rules to allow traffic from ports 80, 443, 9000, and 9001 to access the application.

1. Log in to the FlexusL **console** and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.

The following figure only displays common rules. You can add more rules as needed.

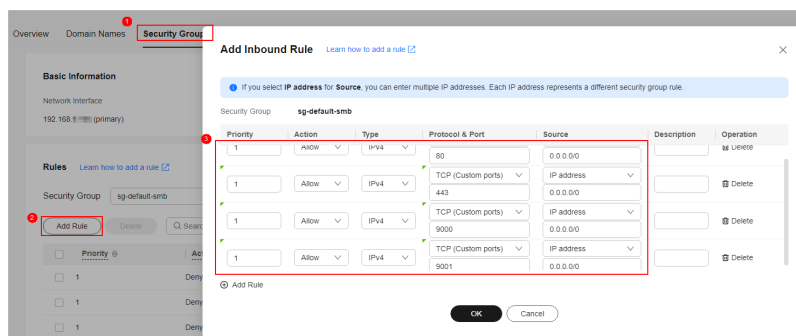
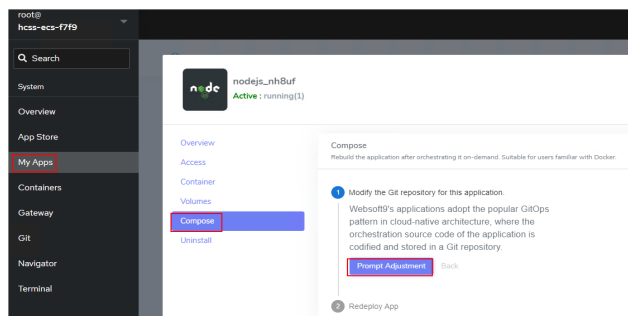


Table 3-2 Security group rules

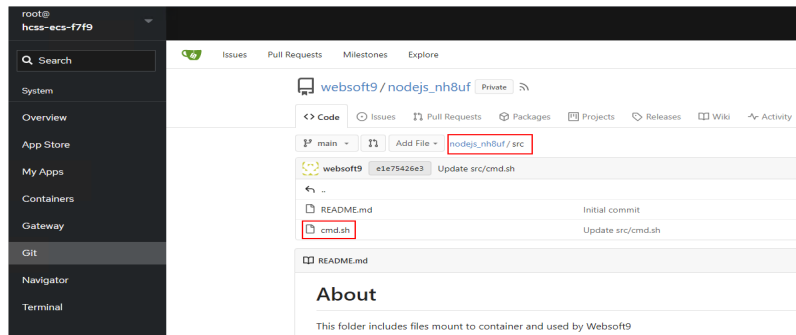
Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of an application.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS traffic to FlexusL instances.
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M page.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

Step 3: Run the Node.js Program

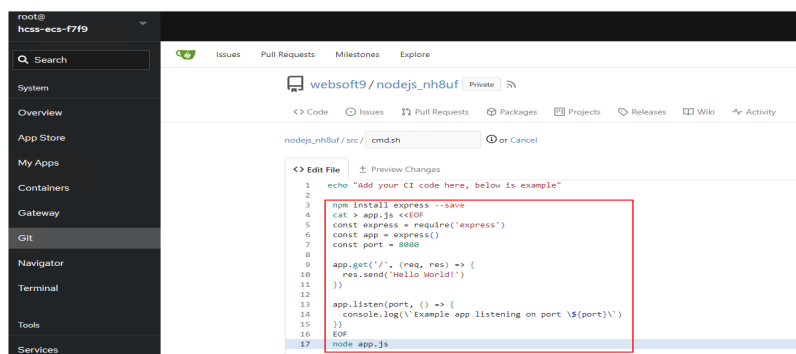
1. In the address bar of a local browser, enter **http://EIP:9000** and enter the username and password to log in to the application O&M page.
 - The username of the O&M page is **root**.
 - The password of the O&M page is the same as that of the FlexusL instance. The FlexusL instance does not have an initial password. Reset the password of the FlexusL instance. For details about how to reset the password, see [Resetting the Password for a FlexusL Instance](#).
2. Choose **My Apps** and click the App icon.
3. Select **Compose** and click **Prompt Adjustment**.



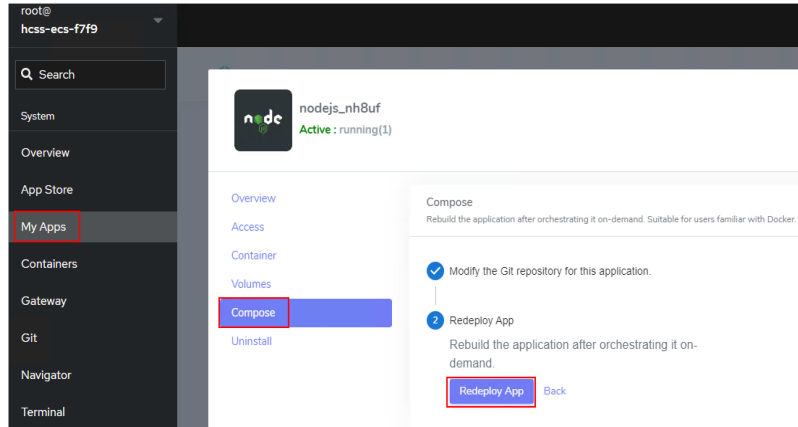
4. On the dashboard, open the **cmd.sh** file in the **src** folder.



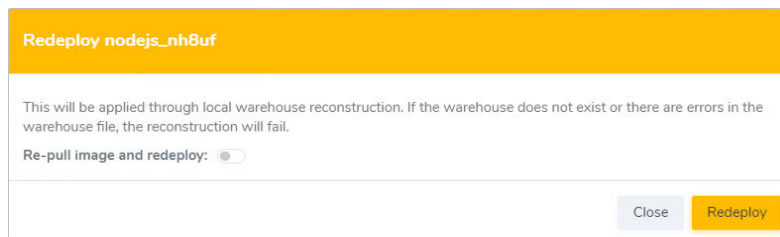
5. After releasing the code in the file, click **Commit Changes** to submit the code.



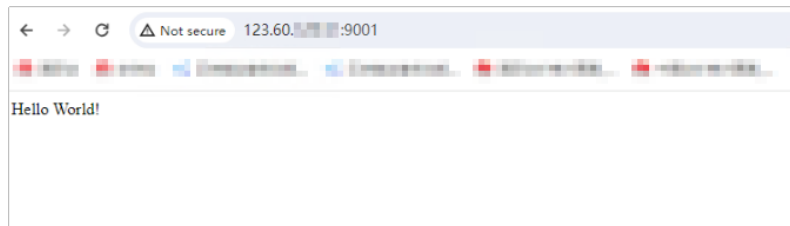
6. On the **Compose** page, click **Redeploy App**.



7. On the displayed page, retain the default settings and click **Redeploy**.



8. In the address bar of a local browser, enter **http://EIP:9001** to check the program execution results.



4 Setting Up an Application

4.1 Project Management Scenarios

4.1.1 Using GitLab to Manage Teams and Projects

Application Scenario

GitLab is a DevOps platform that provides a complete solution for software development and operations, aiming to help teams collaborate on project development. On GitLab, you can protect your applications, and manage, plan, create, validate, package, release, configure, and monitor project source code. Supported By FlexusL, the GitLab image uses Ubuntu 22.04 and is deployed using Docker. The Nginx and Docker have been preconfigured in the image. This section describes how to use GitLab to manage teams and projects.

Resource Planning and Costs

This practice uses the following resource planning as an example. You can adjust it as required.

Resource	Configuration	Description
Cloud server	vCPUs: 2 Memory: 8 GiB	Select appropriate instance specifications based on your service requirements.
Image	GitLab	Select the GitLab application image.
Security group	Inbound rule: <ul style="list-style-type: none">• Protocol/ Application: TCP• Port: 80, 9000, 9001• Source: 0.0.0.0/0	<ul style="list-style-type: none">• 80: Specifies the internal forwarding port of application images.• 9000: Allows external access to the application O&M page.• 9001: Allows external access to the application management page.

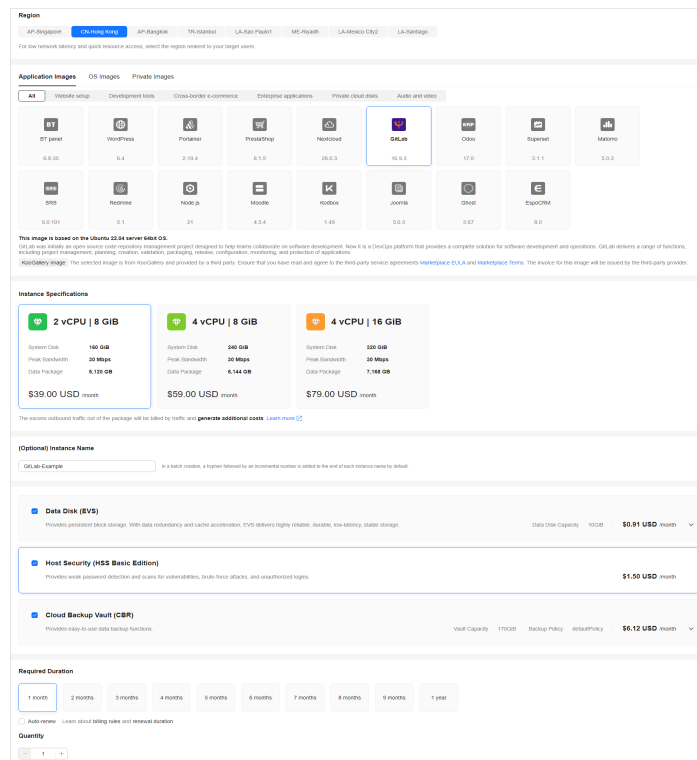
Resource	Configuration	Description
Domain name	wpwebsite.com	<ul style="list-style-type: none">• If the website is only used for personal development or testing, there is no need to add a domain name.• If the website is open to the public, add and resolve a domain name for the cloud server.

Process

Procedure	Description
Step 1: Purchase a FlexusL Instance	Purchase a FlexusL instance and select the GitLab application image.
Step 2: Configure Security Groups	Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.
Step 3: Reset the Password and Log In to the FlexusL Instance	A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance.
Step 4: Initialize GitLab	Log in to GitLab and select the desired language for the management page.
Step 5: Use GitLab	Create a project, add project members, and integrate codes.

Step 1: Purchase a FlexusL Instance

1. Log in to the FlexusL [console](#) and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Application Image	GitLab	Select the GitLab application image.
Instance Specifications	2 vCPUs 8 GiB memory	Select instance specifications as needed.
Instance Name	GitLab-Example	Customize an instance name that is easy to identify, for example, GitLab-Example.
(Optional) Associated Services	<ul style="list-style-type: none"> Data disk: 10 GiB Host security Cloud backup vault: 170 GiB 	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.

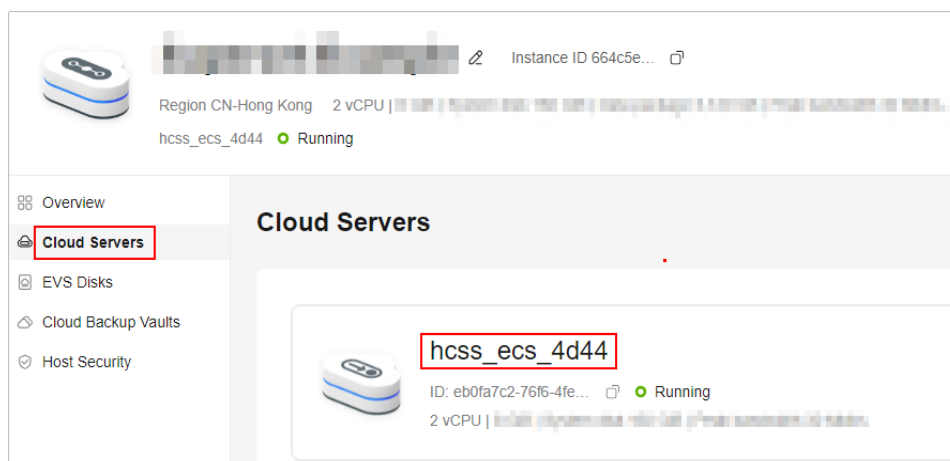
Parameter	Example	Description
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure Security Groups

Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.

The following figure only displays common rules. You can add more rules as needed.

Table 4-1 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of application images
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M page.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

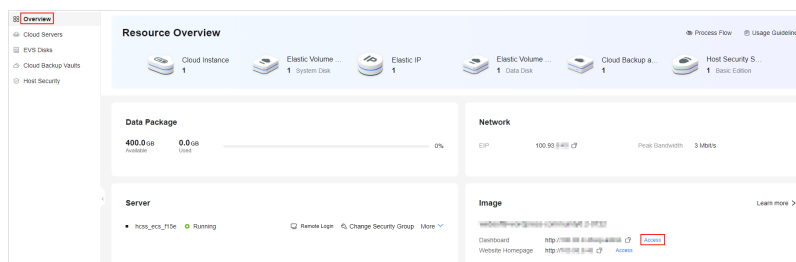
Step 3: Reset a Password

A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance. The password of the FlexusL instance is also used for [logging in to the O&M page of the application](#).

1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard and check whether the application has been up and running. If yes, go to the next step.

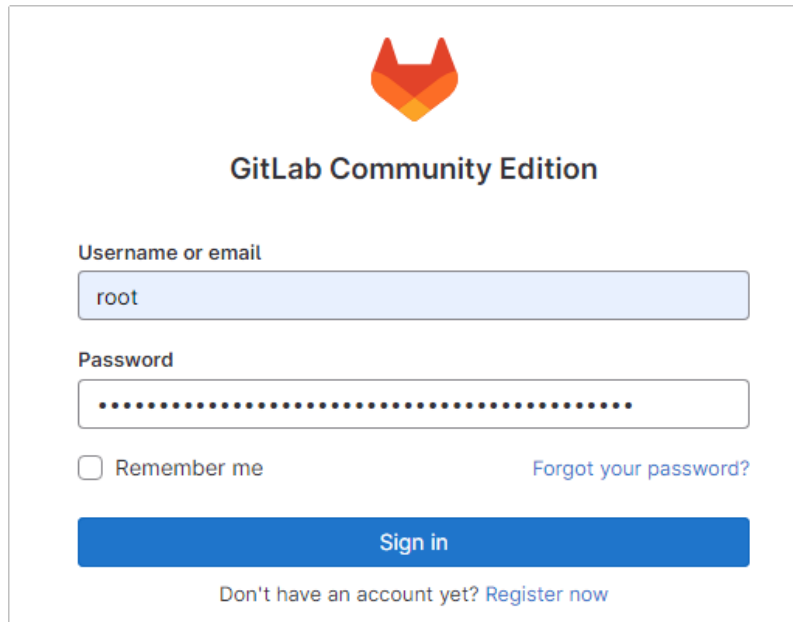
NOTICE

Wait for several minutes until the image with the pre-installed application is up and running. Then, you can perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the initial password may become invalid and you cannot log in to the application dashboard.

Figure 4-1 Entry to the application dashboard

After the application is started, the initialization wizard page of the dashboard is displayed, as shown in [Figure 4-2](#).

Figure 4-2 Initialization wizard page of the GitLab dashboard



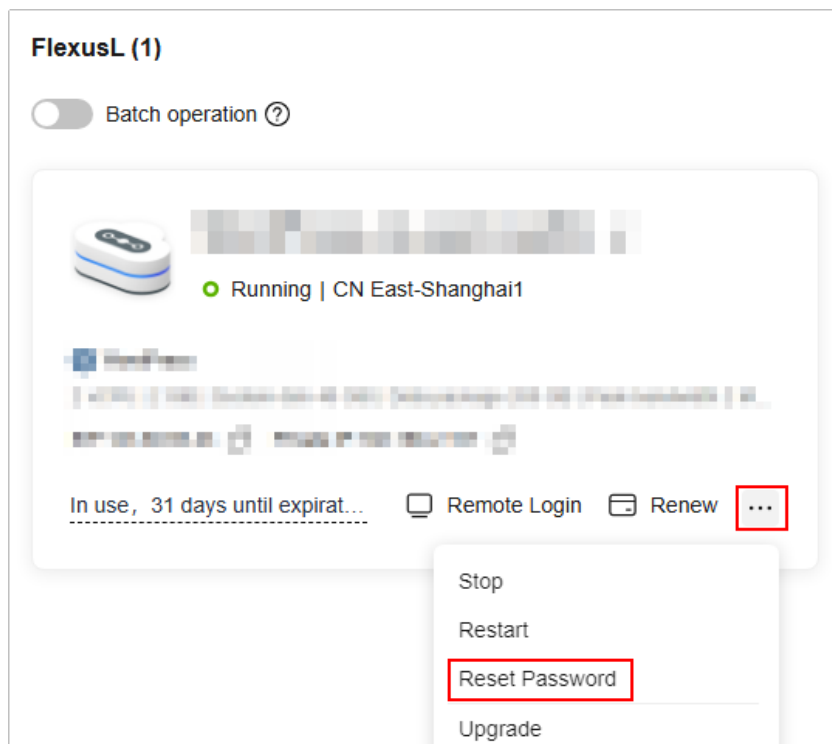
NOTE

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
- The dashboard is being started. Try again later.

2. Locate the resource card and choose **...** > **Reset Password** to reset the password.

For details, see [Resetting the Password for a FlexusL Instance](#).

Figure 4-3 Resetting a password**NOTE**

The password for logging in to the FlexusL instance is also the password for logging in to the O&M page of the application.

Step 4: Initialize GitLab

Application images use code-based Ubuntu. They provide graphical user interfaces to make your operations easier. You need to initialize the application dashboard upon the first login. Then you can directly log in to the dashboard from the FlexusL console afterwards.

1. In the address bar of a local browser, enter **http://<Server-EIP>:9000** to log in to the application O&M page.

The initial username and password for logging in to the application dashboard are stored on the O&M page of the application. You need to log in to the O&M page first to obtain the username and password. The username for logging in to the O&M page is **root**, and the login password is the password reset in **2**.

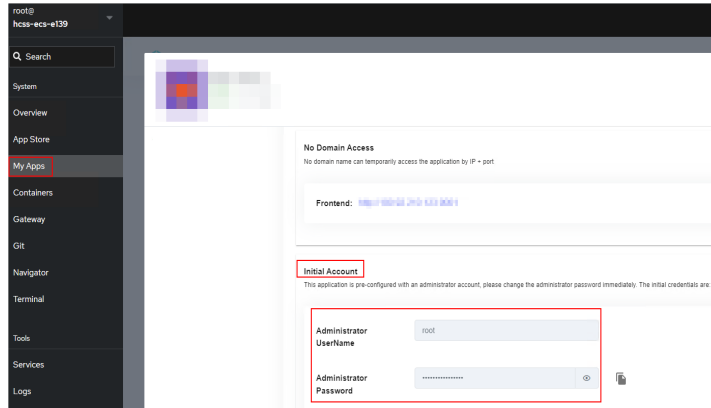
NOTE

For details about the FlexusL instances, O&M page, and dashboard, see [What Is the Relationship Among FlexusL Instances, the Dashboard, and the O&M Page?](#)

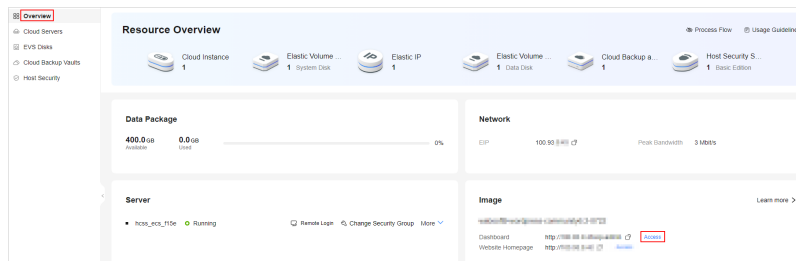
2. On the **My Apps** page, click the application icon, choose **Access**, and click **Initial Account** to view the username and password for logging in to the application management page.

The initial password is a randomly generated strong password. After the application is initialized, change the password on the dashboard for easy

management. If the password is changed, the initial password will be invalid. Remember the new password.



3. On the **Overview** page, click **Access** in the **Dashboard** field in the **Image** area.

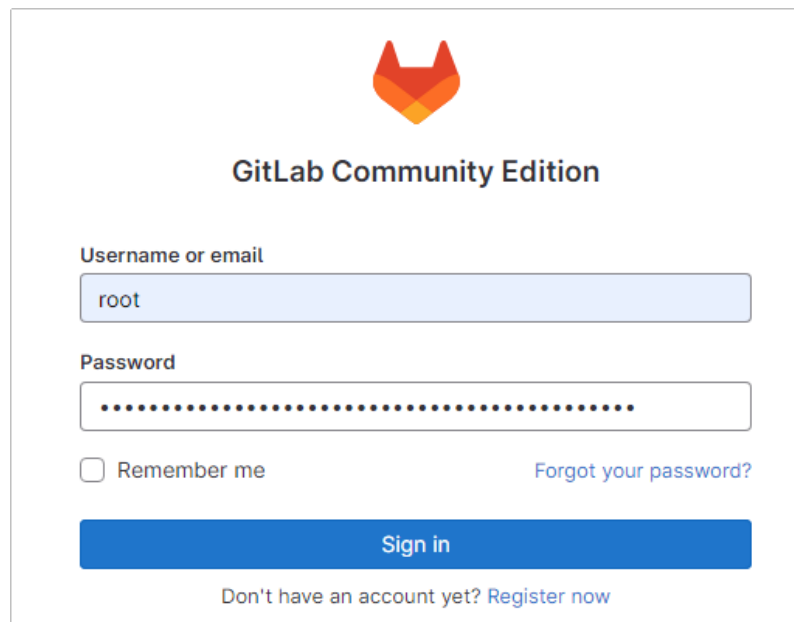


NOTE

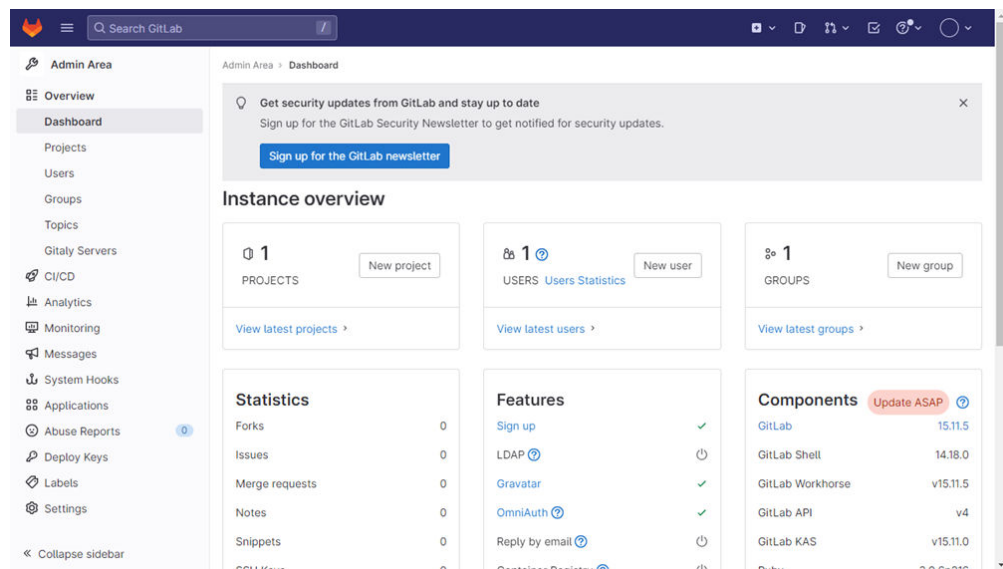
If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
 - The dashboard is being started. Try again later.
4. Enter the username and password obtained in [2](#).

Figure 4-4 Initialization wizard page of the GitLab dashboard



5. Click **Sign in** to access the GitLab Admin Area.




After the GitLab application is initialized, you can create projects on the dashboard.

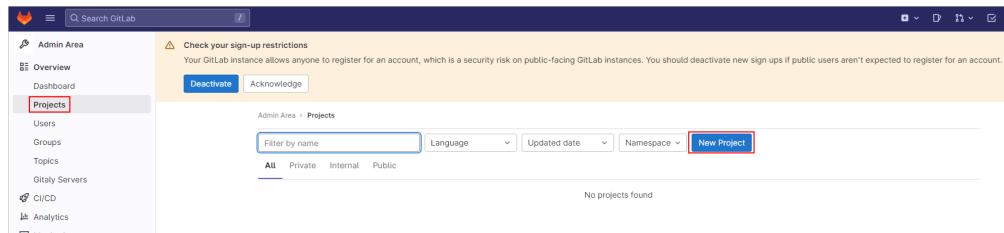
Step 5: Use GitLab

This section describes how to use GitLab to create a project, add project members, and integrate codes.

Step 1: Create a Project

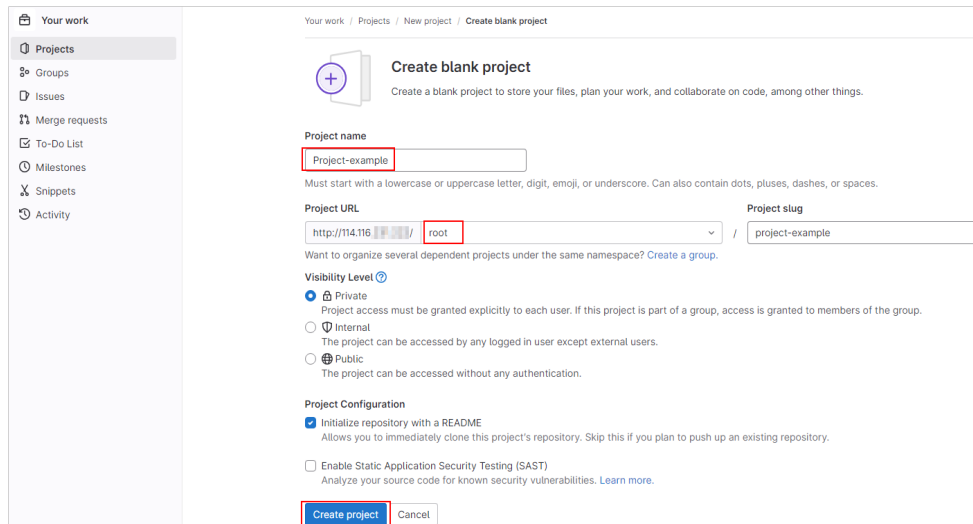
This example demonstrates that how an administrator creates a project, initializes the project, adds a development branch dev, and hides the master branch main from developers.

1. Click  in the upper left corner and choose **admin** to access the management center.
2. Choose **Projects** and click **New project**.

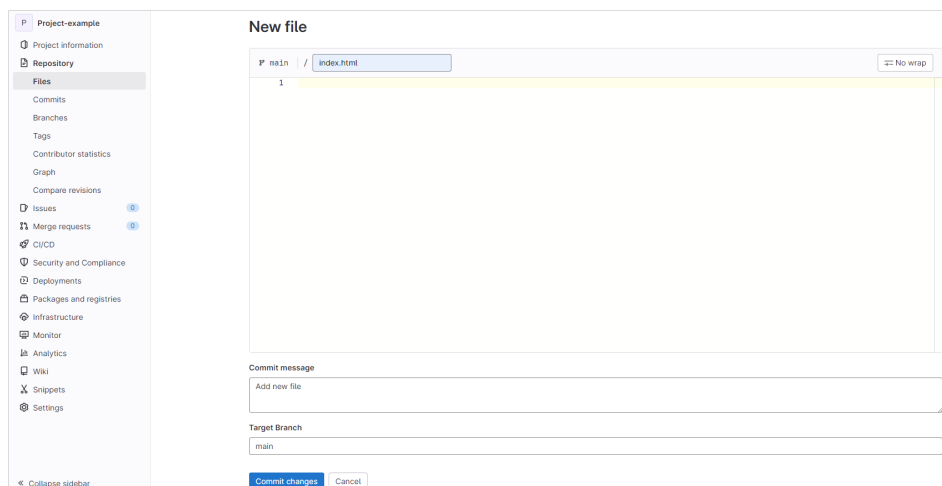


3. Click **Create blank project**.
4. Configure parameters for the project and click **Create project**.
 - **Project name:** Enter a project name that is easy to identify, for example, **Project-example**.
 - **Project URL:** It consists of the public IP address of the cloud service and the administrator account. Select **root**.

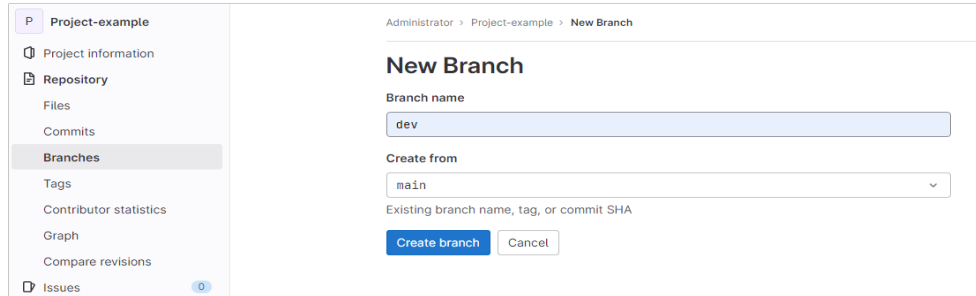
Retain the default values for other parameters.



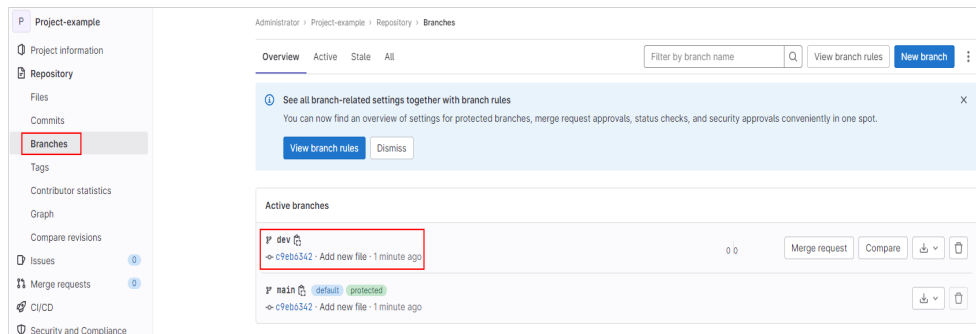
5. Choose **Repository > Files**, click  > **New file**, add the **index.html** file to **main**, and click **Commit changes**.



6. Choose **Repository > Branches**, click **New branch**, and configure the development branch dev.
 - **Branch name:** dev
 - **Create from:** main



7. Click **Create branch**. Then you can view the created development branch dev.



Step 2: Add Project Members

After registering an account, users cannot directly log in to GitLab. To let them log in, the administrator needs to approve their registration, invite them to be members of the project, and assign permissions to them.

1. Register an account.
 - a. Visit `http://public IP address of the server` or `http://domain name`.
 - b. Click **Register now**, enter registration information, and click **Register**.

GitLab Community Edition

First name: Last name:


Username:
Username is available.

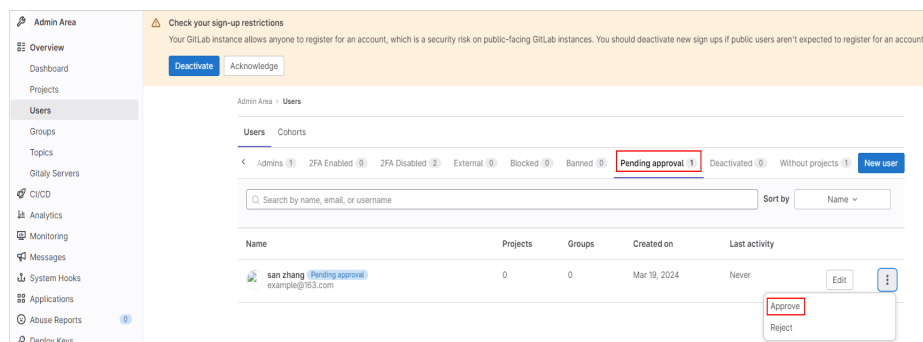
Email:
We recommend a work email address.


Password: Minimum length is 8 characters.

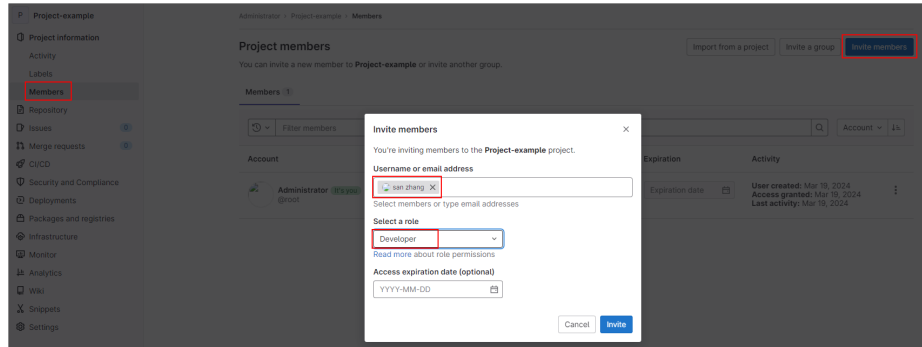
Register

Already have an account? [Sign in](#)

2. The administrator approves the registration.
 - a. Click  in the upper left corner and select **admin**.
 - b. On the **Users** page, select **Pending approval**, and click **Approve**.



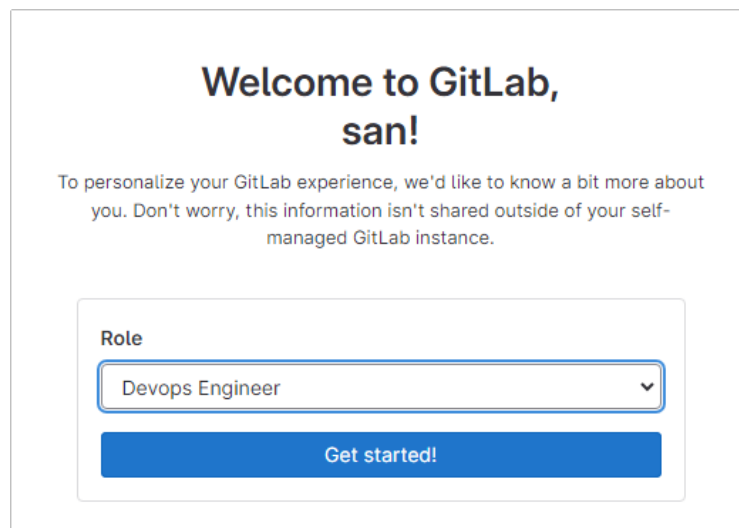
3. The administrator invites users to join the project team and assigns permissions to them.
 - a. Click  in the upper left corner, choose **Projects > View all projects**, and click **Administrator/Project-example**.
 - b. Choose **Project information > Members** and click **Invite members**.
 - c. Enter the username or email address, assign **Developer** permission to users, and click **Invite**.



You can assign users the following five roles: **Guest**, **Reporter**, **Developer**, **Maintainer**, or **Owner**.

- **Guest:** allows users to create issues and post comments, and denies them to read or write the repository.
 - **Reporter:** allows users to clone codes, and denies them to submit code.
 - **Developer:** allows users to clone, develop, submit, and push code.
 - **Master:** allows users to create projects, add tags, protect branches, add new members to the project, and edit projects.
 - **Owner:** allows users to assign permissions to access projects, delete or migrate projects, and manage project team members.
4. Visit <http://Public IP address of the server> or <http://Domain name>. Enter the username and password to log in to GitLab.

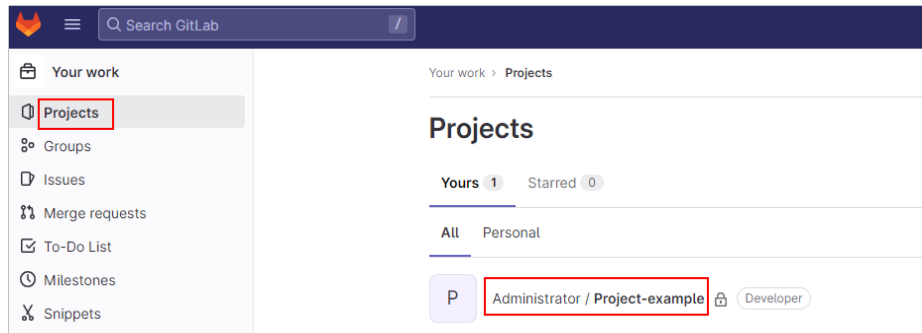
When members log in to GitLab for the first time, select a role for better experience.



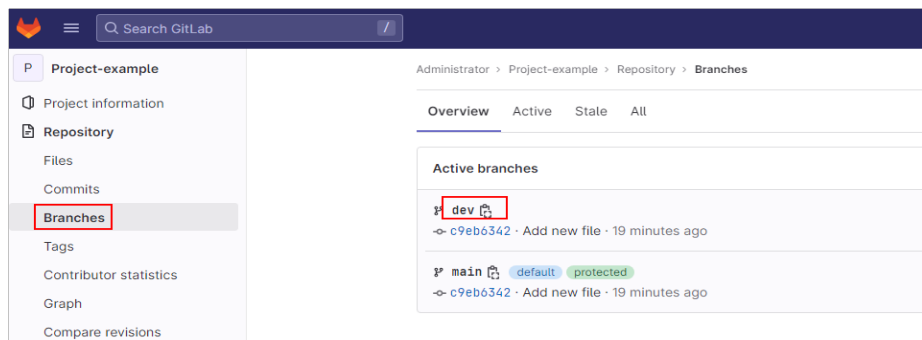
Step 3: Integrate Codes

1. The developers edit and submit code.
 - a. Visit <http://Public IP address of the server> or <http://Domain name> to log in to GitLab.

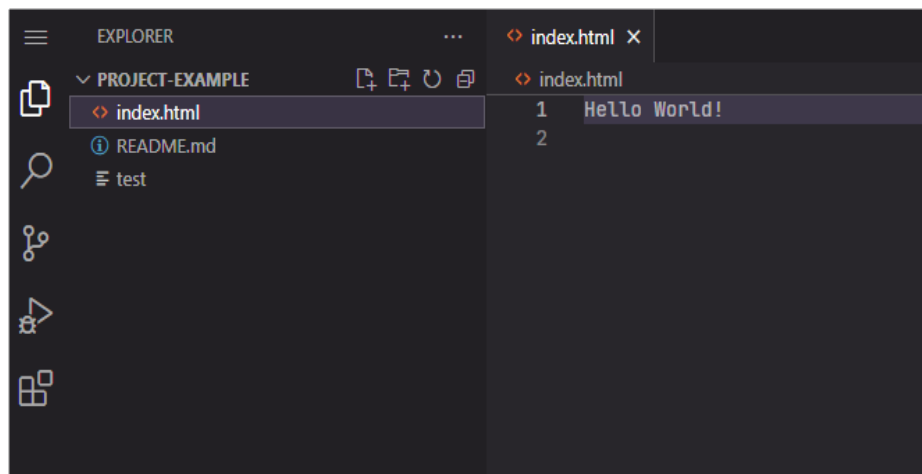
- b. Choose **Projects** and click the target project name.




- c. Choose **Repository > Branch** and click **dev**.

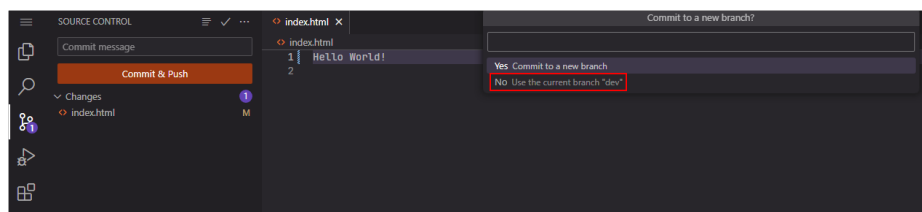


- d. Click **Web IED**, select a file to edit. For example, edit the index.html file.

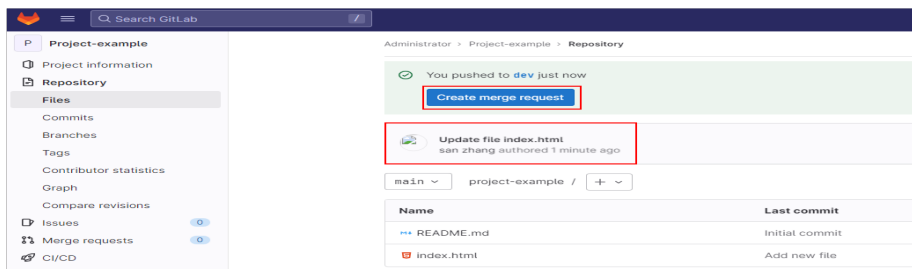


- e. Choose  on the left navigation pane to go to the **SOURCE CONTROL**, and click **Commit & Push**.

Click **No** when **Commit to a new branch?** is displayed.

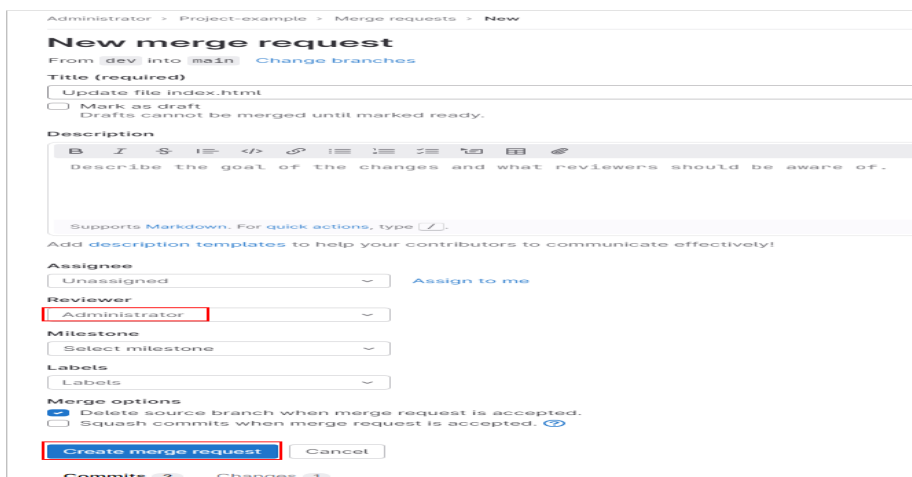


- f. Choose **Repository > Files** on the project menu bar. You can view **Update file index.html**. Click **Create merge request**




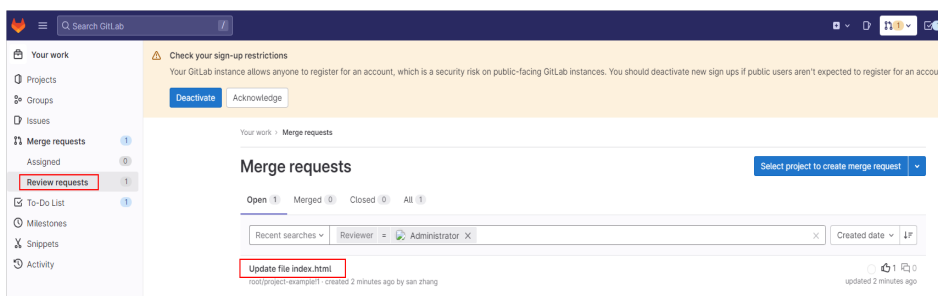
- g. Set request information and click **Create merge request**.

Specify the **Reviewer** to **Administrator** and retain the default values for other parameters.



- 2. The administrator reviews the merge request.

- a. Click  in the upper right corner, choose **Merge requests > New merge request**, and click the specific request title.



- b. Click **Merge** to merge the index.html file from **dev** into **main**.

4.1.2 Using Redmine to Create a Project

Application Scenario

Redmine is an open-source project management software. It provides functions such as project management, Wiki, and news, and integrates tools such as GIT, SVN, and CVS. The Redmine application image uses the Ubuntu 22.04 and is deployed using Docker. The Redmine application and the required operating environment have been preconfigured. This section describes how to use the Redmine application image to create a project.

Resource Planning and Costs

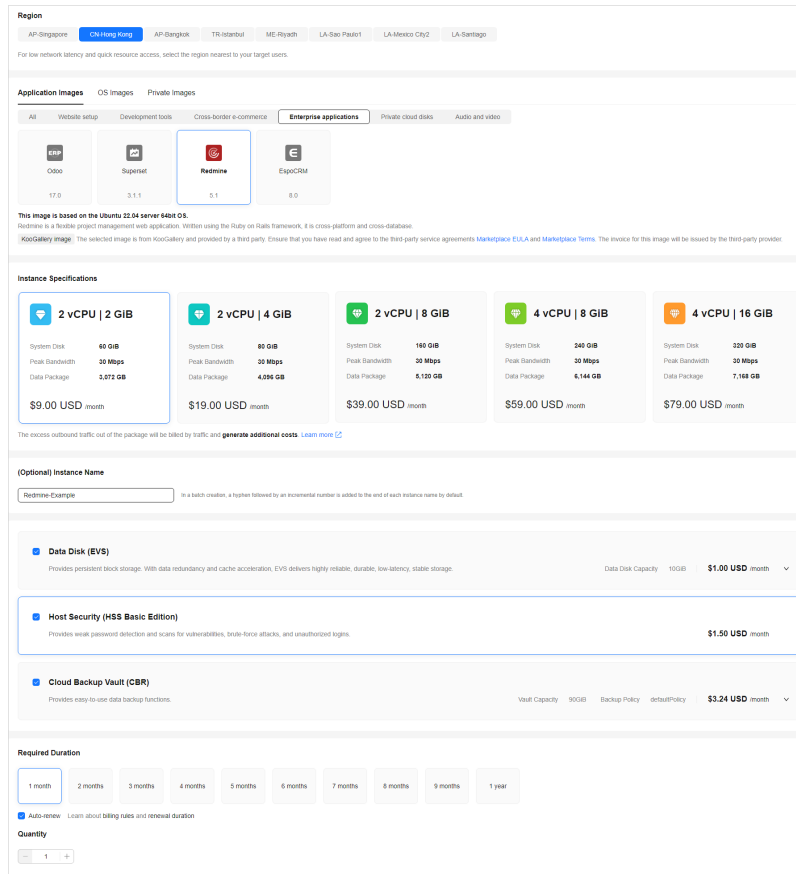
Resource	Configuration	Description
Cloud server	<ul style="list-style-type: none">vCPUs: 2Memory: 2 GiB	Select appropriate instance specifications based on your service requirements.
Image	Redmine	Select the Redmine application image.
Security group	Inbound rule: <ul style="list-style-type: none">Protocol/ Application: TCPPort: 80, 443, 9000, or 9001Source: 0.0.0.0/0	<ul style="list-style-type: none">80: Specifies the internal forwarding port of an application.443: Allows HTTPS traffic to FlexusL instances.9001: Allows external access to the application dashboard.9000: Allows external access to the application O&M page.

Process

Procedure	Description
Step 1: Purchase FlexusL Instances	Purchase a FlexusL instance and select the Redmine application image.
Step 2: Configure Security Groups	Add inbound security group rules to allow traffic from ports 80, 443, 9000, and 9001 to access the application.
Step 3: Reset a Password	A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance.
Step 4: Initialize Redmine	The image application dashboard needs to be initialized only when you log in for the first time.
Step 5: Create a Project	Use the Redmine application image to create a project.

Step 1: Purchase FlexusL Instances

1. Log in to the FlexusL [console](#) and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Application Image	Redmine	Select the Redmine application image.
Instance Specifications	2 vCPUs 2 GiB System disk 60 GiB	Select instance specifications as needed.
Instance Name	Redmine-Example	Customize an instance name that is easy to identify, for example, Redmine-Example.

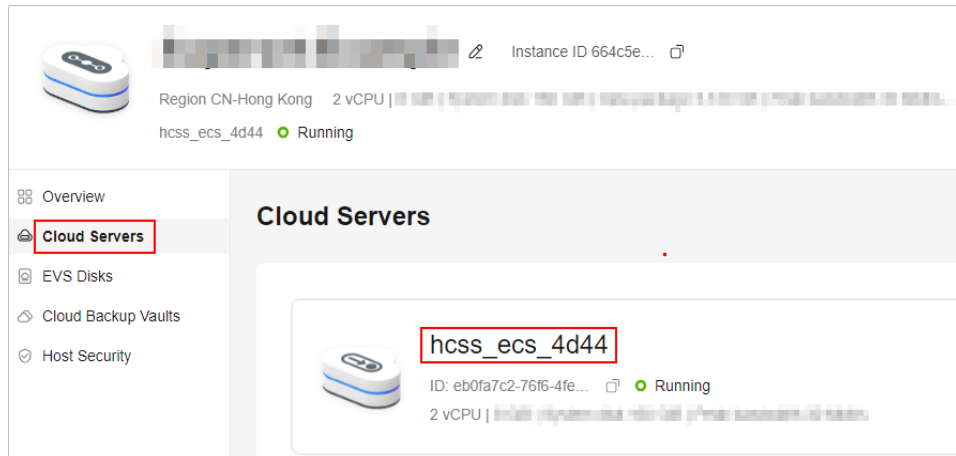
Parameter	Example	Description
(Optional) Associated Service	<ul style="list-style-type: none">• Data Disk: 10 GiB• Host Security• Cloud Backup Vault: 70 GiB	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure Security Groups

Add inbound security group rules to allow traffic from ports 80, 443, 9000, and 9001 to access the application.

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.

The following figure only displays common rules. You can add more rules as needed.

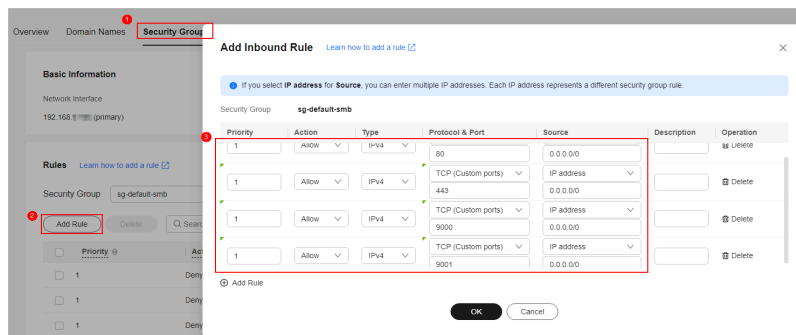


Table 4-2 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of an application.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS traffic to FlexusL instances.
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M page.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

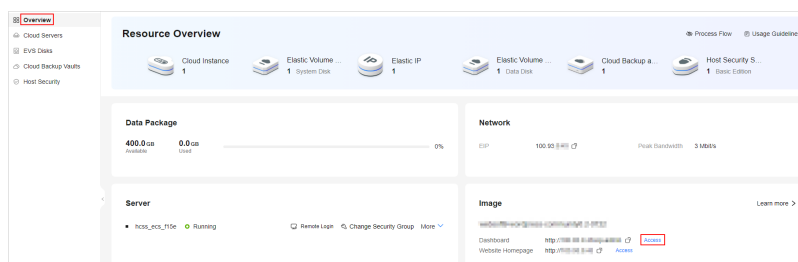
Step 3: Reset a Password

A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance. The password of the FlexusL instance is also used for **logging in to the O&M page of the application**.

1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard and check whether the application has been up and running. If yes, go to the next step.

NOTICE

Wait for several minutes until the image with the pre-installed application is up and running. Then, you can perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the initial password may become invalid and you cannot log in to the application dashboard.

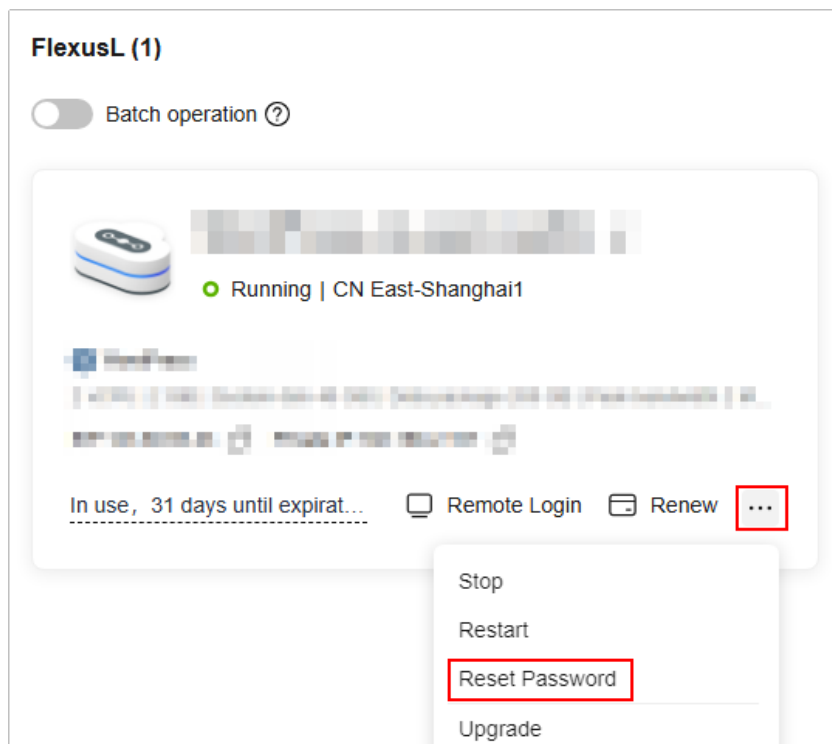
Figure 4-5 Entry to the application dashboard

After the application is started, the initialization wizard page of the dashboard is displayed.

NOTE

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
 - The dashboard is being started. Try again later.
2. Locate the resource card and choose ******* > **Reset Password** to reset the password.
For details, see [Resetting the Password for a FlexusL Instance](#).

Figure 4-6 Resetting a password**NOTE**

The password for logging in to the FlexusL instance is also the password for logging in to the O&M page of the application.

Step 4: Initialize Redmine

Application images use code-based Ubuntu. They provide graphical user interfaces to make your operations easier. You need to initialize the application dashboard upon the first login. Then you can directly log in to the dashboard from the FlexusL console afterwards.

1. In the address bar of a local browser, enter **http://<Server-EIP>:9000** to log in to the application O&M page.

The initial username and password for logging in to the application dashboard are stored on the O&M page of the application. You need to log in to the O&M page first to obtain the username and password. The username for logging in to the O&M page is **root**, and the login password is the password reset in **2**.

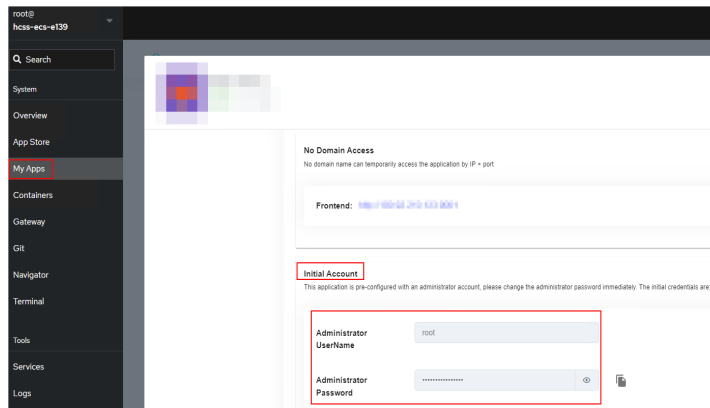
NOTE

For details about the FlexusL instances, O&M page, and dashboard, see [What Is the Relationship Among FlexusL Instances, the Dashboard, and the O&M Page?](#)

2. On the **My Apps** page, click the application icon, choose **Access**, and click **Initial Account** to view the username and password for logging in to the application management page.

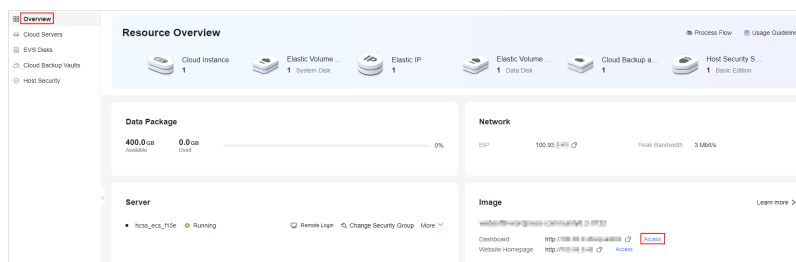
The initial password is a randomly generated strong password. After the application is initialized, change the password on the dashboard for easy

management. If the password is changed, the initial password will be invalid. Remember the new password.



3. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard.

Figure 4-7 Entry to the application dashboard



NOTE

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
 - The dashboard is being started. Try again later.
4. In the upper right corner, click **Log in**. On the displayed login page, enter the initial username and password obtained in [2](#) and click **Log in**.

NOTE

If a message is displayed indicating that the username or password you entered is invalid when you attempt to log in to the application dashboard, refer to [Why Can't I Access the Dashboard of the Application Pre-installed in the Application Image After Entering the Initial Username and Password?](#)

5. On the dashboard, change the password as prompted and click **Apply**.

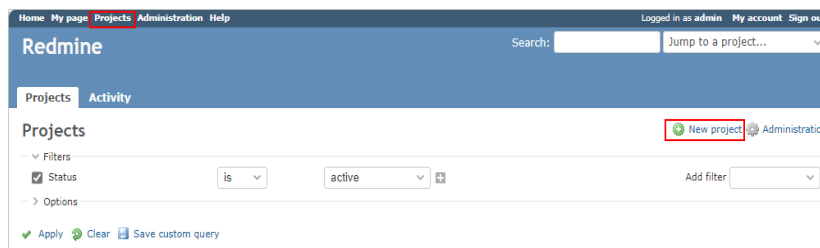
NOTE

If the password is changed, the initial password will be invalid. Remember the new password.

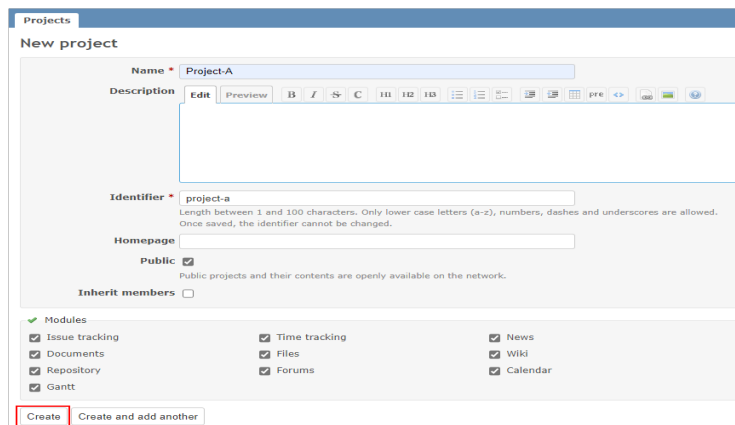
After the Redmine application is initialized, you can create projects on the dashboard.

Step 5: Create a Project

1. Click **Projects** in the upper left corner. In the upper right corner of the page, click **New project** to create a project.

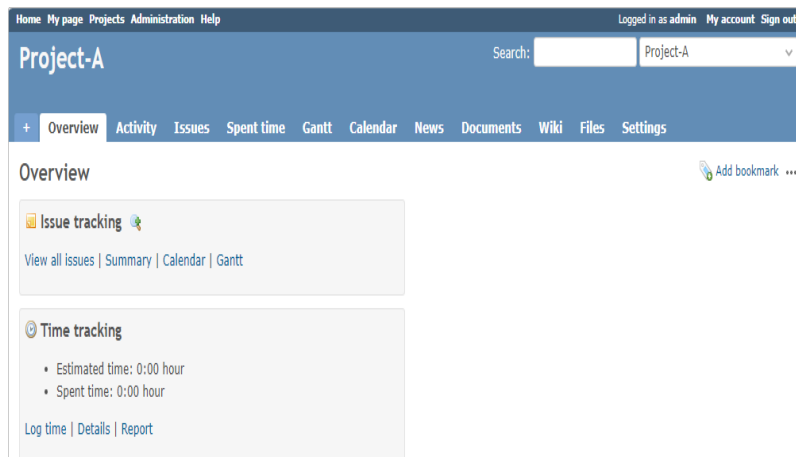


2. Enter the project name and description and click **Create**.



3. Manage projects.

After a project is created, multiple tab pages for project management are displayed. You can use various functions to manage your projects.



4.2 Cloud Disk Scenarios

4.2.1 Using Nextcloud to Set Up an Enterprise Web Disk System

Application Scenario

Nextcloud is a suite of open-source cloud based storage software for self-built private cloud disks for enterprises. Nextcloud supports PC, Android, and iOS, and you can easily synchronize with vital data stored on servers, including files, schedules, contacts, and bookmarks. Supported By FlexusL, the Nextcloud image uses Ubuntu 22.04 and is deployed using Docker. The Nginx, MySQL, phpMyAdmin, and Docker have been preconfigured in the image. This section describes how to use Nextcloud to build an enterprise web disk system.

Resource Planning and Costs

This practice uses the following resource planning as an example. You can adjust it as required.

Resource	Configuration	Description
Cloud server	<ul style="list-style-type: none">vCPUs: 2Memory: 4 GiB	Select appropriate instance specifications based on your service requirements.
Image	Nextcloud	Select the Nextcloud application image.
Security group	Inbound rule: <ul style="list-style-type: none">Protocol & Port TCP: 80,9000,9001 Source: 0.0.0.0/0Protocol & Port ICMP: all Source: 0.0.0.0/0	<ul style="list-style-type: none">80: Specifies the internal forwarding port of application images.9000: Allows external access to the application O&M page.9001: Allows external access to the application management page.
Domain name	wpwebsite.com	<ul style="list-style-type: none">If the website is only used for personal development or testing, there is no need to add a domain name.If the website is open to the public, add and resolve a domain name for the cloud server.

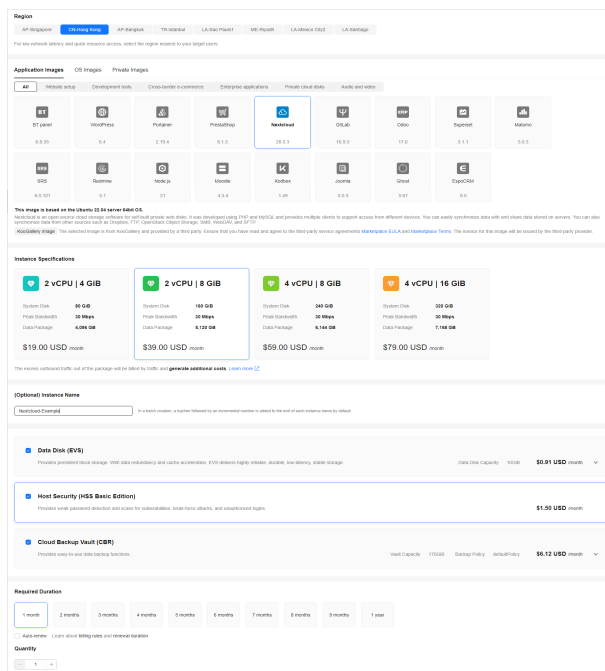
Process

Procedure	Description
Step 1: Purchase a FlexusL Instance	Purchase a FlexusL instance and select the Nextcloud application image.

Procedure	Description
Step 2: Configure Security Groups	Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.
Step 3: Reset the Password and Log In to the FlexusL Instance	A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance.
Step 4: Initialize Nextcloud	Log in to the frontend page and install Nextcloud.
Step 5: Deploy Nextcloud	On the dashboard, perform the following operations: <ul style="list-style-type: none"> • Install applications • Configure SMTP

Step 1: Purchase a FlexusL Instance

1. Log in to the FlexusL console and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.

Parameter	Example	Description
Application Image	Nextcloud	Select the Nextcloud application image.
Instance Specifications	2 vCPUs 4 GiB memory and 80 GiB system disk	Select instance specifications as needed.
Instance Name	Nextcloud-Example	Customize an instance name that is easy to identify, for example, Nextcloud-Example.
(Optional) Associated Services	<ul style="list-style-type: none">• Data Disk: 10 GiB• Host Security• Cloud backup vault: 90 GiB	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

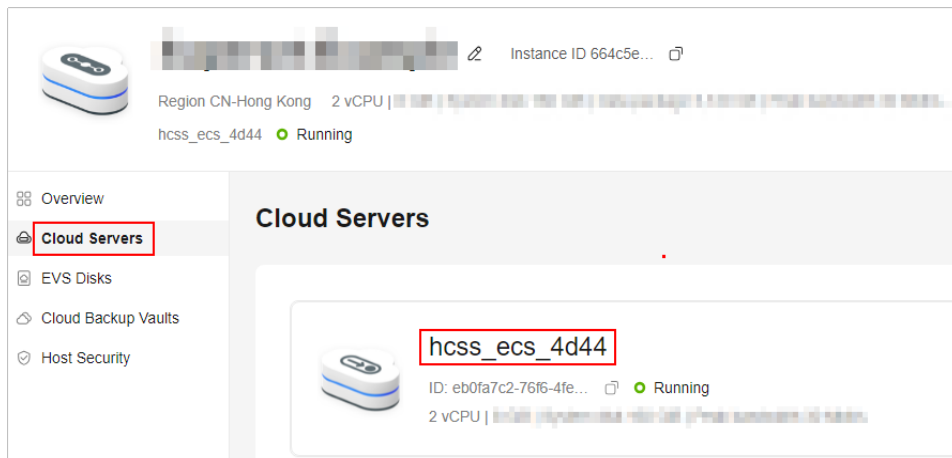
3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure Security Groups

Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.

2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.
The following figure only displays common rules. You can add more rules as needed.

Table 4-3 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of application images
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M page.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

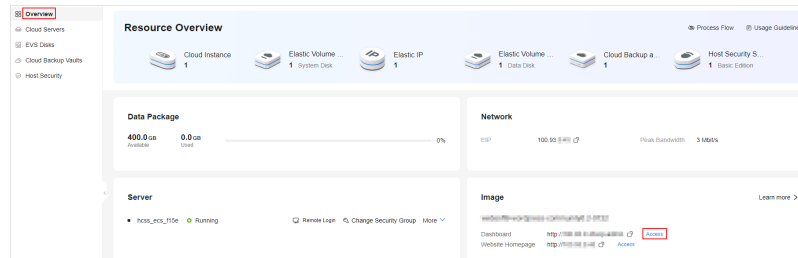
Step 3: Reset a Password

A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance. The password of the FlexusL instance is also used for [logging in to the O&M page of the application](#).

1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard and check whether the application has been up and running. If yes, go to the next step.

NOTICE

Wait for several minutes until the image with the pre-installed application is up and running. Then, you can perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the initial password may become invalid and you cannot log in to the application dashboard.

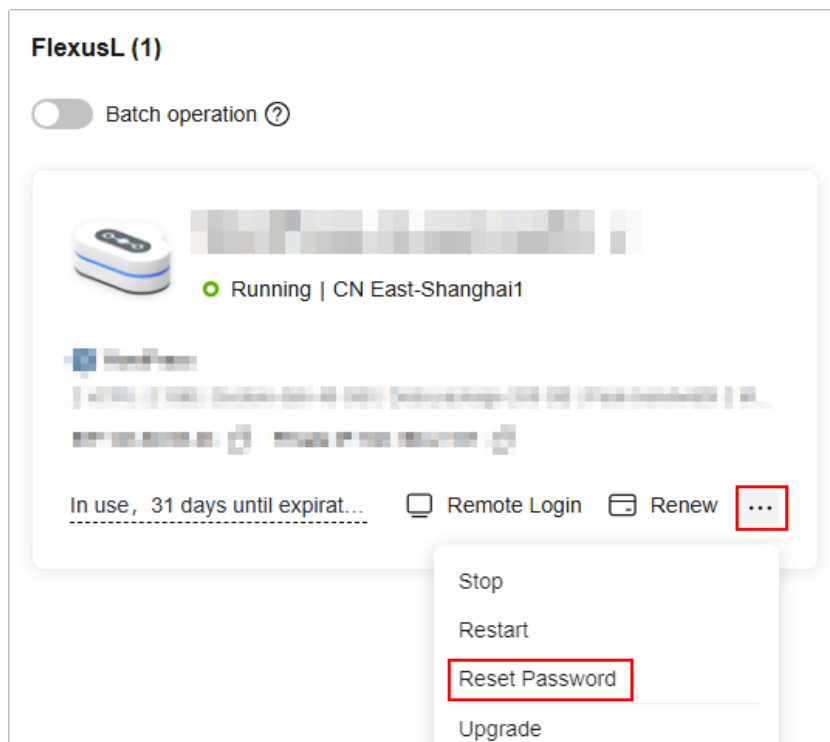
Figure 4-8 Entry to the application dashboard**NOTE**

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
- The dashboard is being started. Try again later.

2. Locate the resource card and choose ******* > **Reset Password** to reset the password.

For details, see [Resetting the Password for a FlexusL Instance](#).

Figure 4-9 Resetting a password**NOTE**

The password for logging in to the FlexusL instance is also the password for logging in to the O&M page of the application.

Step 4: Initialize Nextcloud

Application images use code-based Ubuntu. They provide graphical user interfaces to make your operations easier. You need to initialize the application dashboard upon the first login. Then you can directly log in to the dashboard from the FlexusL console afterwards.

1. In the address bar of a local browser, enter **http://<Server-EIP>:9000** to log in to the application O&M page.

The initial username and password for logging in to the application dashboard are stored on the O&M page of the application. You need to log in to the O&M page first to obtain the username and password. The username for logging in to the O&M page is **root**, and the login password is the password reset in **Step 3: Reset a Password**.

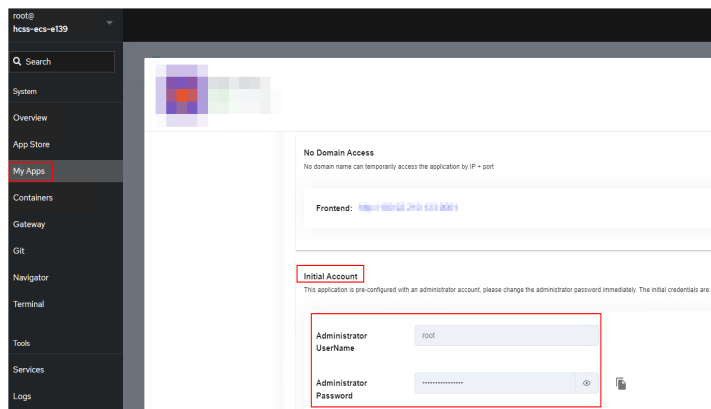
NOTE

For details about the FlexusL instances, O&M page, and dashboard, see **What Is the Relationship Among FlexusL Instances, the Dashboard, and the O&M Page?**

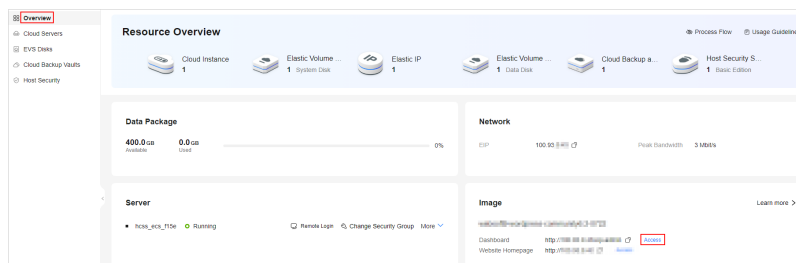
2. On the **My Apps** page, click the application icon, choose **Access**, and click **Initial Account** to view the username and password for logging in to the application management page.

The initial password is a randomly generated strong password. After the application is initialized, change the password on the dashboard for easy

management. If the password is changed, the initial password will be invalid. Remember the new password.



3. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard.



NOTE

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
- The dashboard is being started. Try again later.

4. Enter the username and password obtained in 2. Click **Log in**.

NOTE

If a message is displayed indicating that the username or password you entered is invalid when you attempt to log in to the application dashboard, refer to [Why Can't I Access the Dashboard of the Application Pre-installed in the Application Image After Entering the Initial Username and Password?](#)

5. After the installation is complete, you can continue to install recommended applications as prompted or click **Cancel**.
You can still install these applications on the management page subsequently.
6. You can go through the pop-ups to learn about the Nextcloud functions, and then configure Nextcloud on the management page.


After the Nextcloud application is initialized, you can deploy your applications on the dashboard.

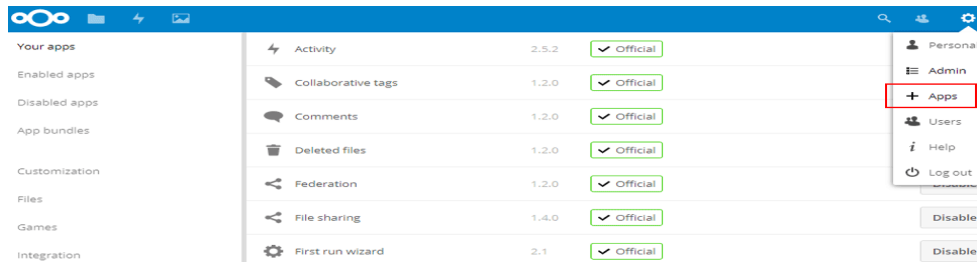
Step 5: Deploy Nextcloud

This section describes some basic operations of Nextcloud. For details, see [Nextcloud Documentation](#).

Installing Applications


Nextcloud integrates various applications, and you can add more functions to Nextcloud by installing these applications.

1. Click  in the upper right corner and choose **Apps** to view the applications integrated with Nextcloud.
2. Click **Enable**.



Configuring SMTP

Configuring an SMTP mail server in an application is very important. It can be used to get back your passwords and receive important notifications. You are advised to configure the SMTP service to enable the email notification function.

1. Click  in the upper right corner and click **Personal**.
2. Enter the sender's email address, for example, example@163.
The email address must be available, and the SMTP function must have been configured.
3. Choose **Administration > Basic Settings > Email Server**, and configure SMTP information.

In this example, the 163 mailbox is only for reference. Please configure the corresponding parameters when other mailboxes are used.

Email server *i*

It is important to set up this server to be able to send emails, like for password reset and notifications.

Send mode	SMTP	Encryption	SSL/TLS
From address	example	@	163.com
Authentication method	Login	<input checked="" type="checkbox"/>	Authentication required
Server address	smtp.163.com	:	465
Credentials	example@163.com	SMTP Password	Store credentials

Test email settings

Parameter	Description
Send mode	Select SMTP.
Encryption	Select SSL/TLS.
From address	Enter an email address, for example, example@163.com.
Server address	Enter smtp.163.com for the 163 email server.
Port number	Enter 465.
Authentication method	Select Authentication required .
Credentials	<ul style="list-style-type: none">• SMTP Username: Set it to the email address.• SMTP Password: Set it to the authorization code obtained when configuring SMTP for example@163.com rather than the login password of example@163.com.

4. Click **Store credentials**.
5. Click **Send email** to test whether the SMTP has been successfully configured.

4.2.2 Using Kodbox to Quickly Set Up a Cloud Disk

Application Scenario

Kodbox is an open-source system that integrates online file management, multi-cloud storage, and collaborative office. The Kodbox application image uses the Ubuntu 22.04 and is deployed using Docker. The Kodbox application and the required operating environment have been preconfigured. This section describes how to use the Kodbox application image to quickly set up a cloud disk.

Resource Planning and Costs

Resource	Configuration	Description
Cloud server	<ul style="list-style-type: none">• vCPUs: 2• Memory: 2 GiB	Select appropriate instance specifications based on your service requirements.
Image	Kodbox	Select the Kodbox application image.
Security group	Inbound rule: <ul style="list-style-type: none">• Protocol/ Application: TCP• Port: 80, 443, 9000, or 9001• Source: 0.0.0.0/0	<ul style="list-style-type: none">• 80: Specifies the internal forwarding port of an application.• 443: Allows HTTPS traffic to FlexusL instances.• 9001: Allows external access to the application dashboard.• 9000: Allows external access to the application O&M page.

Process

Procedure	Description
Step 1: Purchase FlexusL Instances	Purchase a FlexusL instance and select the Kodbox application image.
Step 2: Configure Security Groups	Add inbound security group rules to allow traffic from ports 80, 443, 9000, and 9001 to access the application.
Step 3: Initialize Kodbox.	The image application dashboard needs to be initialized only when you log in for the first time.
Step 4: Deploy a Cloud Disk	Deploy an application on the visualization application management page.

Step 1: Purchase FlexusL Instances

1. Log in to the FlexusL [console](#) and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.

The screenshot displays the 'Purchase FlexusL Instance' configuration page. At the top, the 'Region' is set to 'CN-Hong Kong'. Under 'Application Images', the 'Kodbox' image is selected. The 'Instance Specifications' section offers five options, with '2 vCPU | 2 GIB' selected. Below this, optional add-ons are shown: 'Data Disk (EVS)' for \$1.00/month, 'Host Security (HSS Basic Edition)' for \$1.50/month, and 'Cloud Backup Vault (CBR)' for \$2.52/month. The 'Required Duration' is set to '1 month' and the 'Quantity' is '1'.

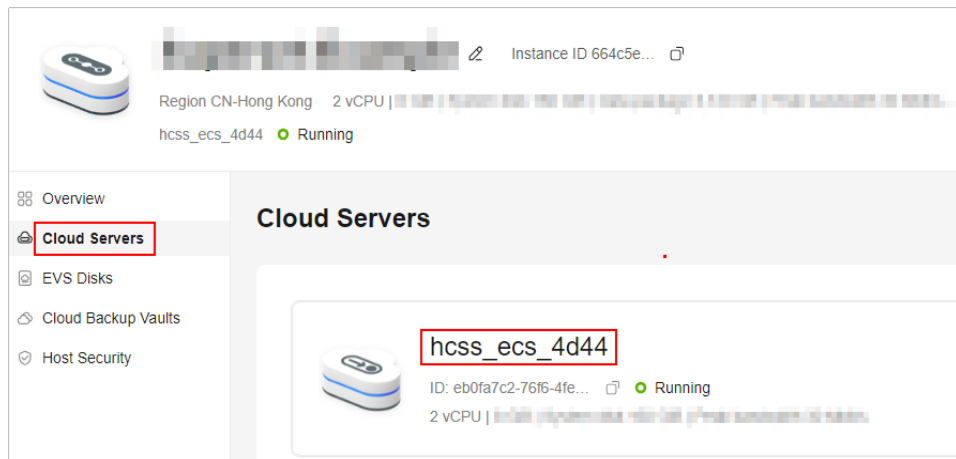
Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Application Image	Kodbox	Select the Kodbox application image.
Instance Specifications	2 vCPU 2 GiB System disk 60 GiB	Select instance specifications as needed.
Instance Name	Kodbox-Example	Customize an instance name that is easy to identify, for example, Kodbox-Example.
(Optional) Associated Service	<ul style="list-style-type: none">• Data Disk: 10 GiB• Host Security• Cloud Backup Vault: 70 GiB	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure Security Groups

Add inbound security group rules to allow traffic from ports 80, 443, 9000, and 9001 to access the application.

1. Log in to the FlexusL **console** and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.

The following figure only displays common rules. You can add more rules as needed.

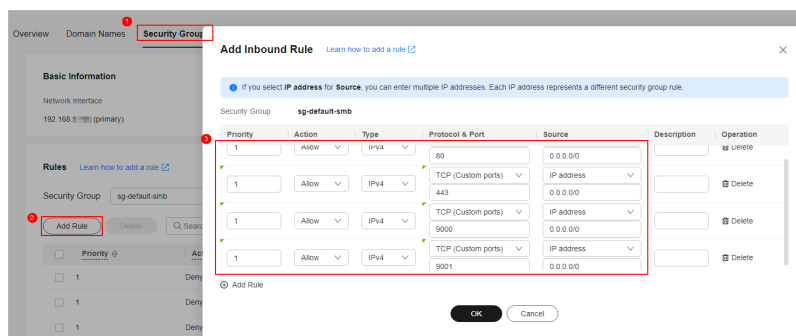


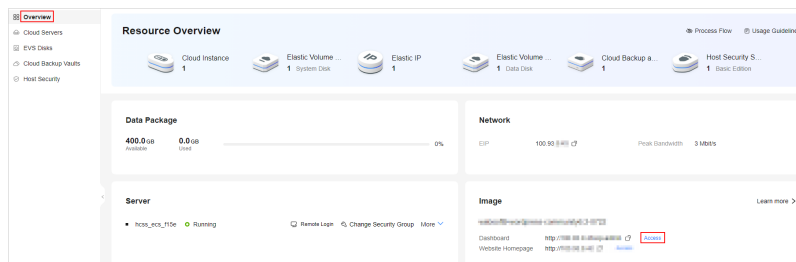
Table 4-4 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of an application.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS traffic to FlexusL instances.
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M page.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

Step 3: Initialize Kodbox.

Application images use code-based Ubuntu. They provide graphical user interfaces to make your operations easier. You need to initialize the application dashboard upon the first login. Then you can directly log in to the dashboard from the FlexusL console afterwards.

1. On the **Overview** page, click **Access** in the **Dashboard** field in the **Image** area.

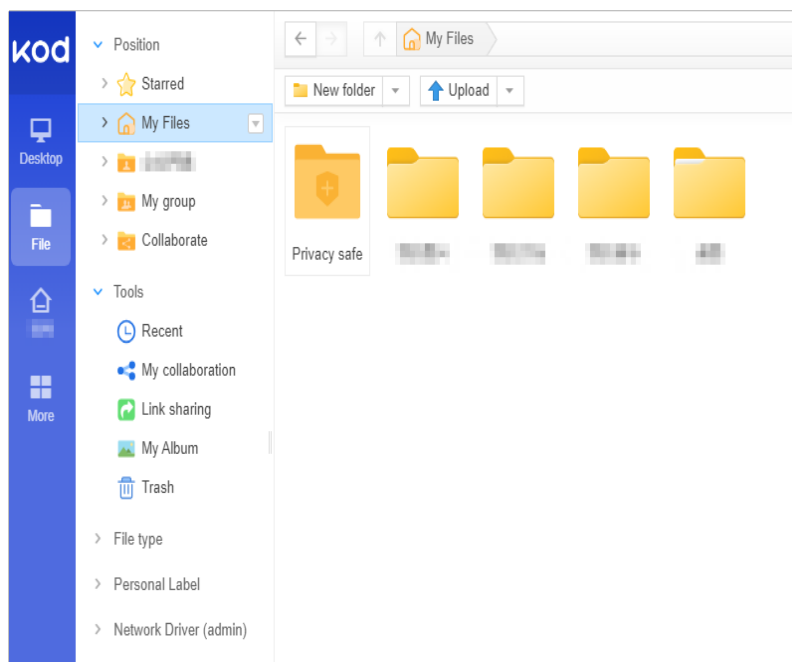


NOTE

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
 - The dashboard is being started. Try again later.
2. Set the account and password for logging in to the dashboard and click **OK**. Kodbox does not have a default username or password. Set a username and password that are easy to remember.
 3. Enter the username and password for logging in to the dashboard, and click **Log in**.
 4. Check the application dashboard.

After logging in to the application management page, information similar to the following is displayed.



After the Kodbox application is initialized, you can deploy your applications on the dashboard.

Step 4: Deploy a Cloud Disk

For details about how to deploy a Kodbox cloud disk, see [Kodbox Service Support](#).

4.3 E-commerce

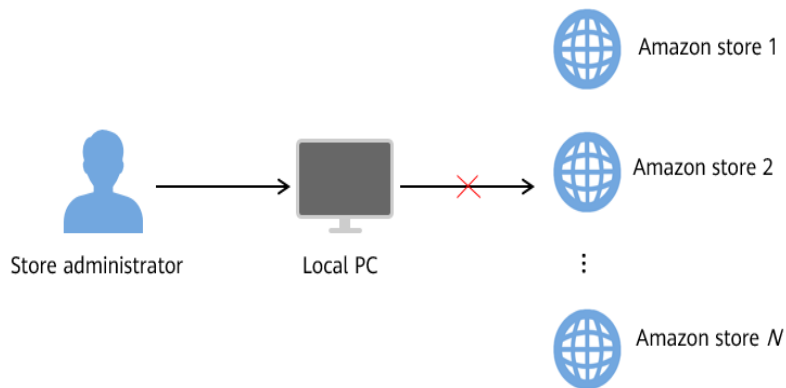
4.3.1 Using Windows Server to Set Up a Cross-Border E-Commerce Store

Application Scenario

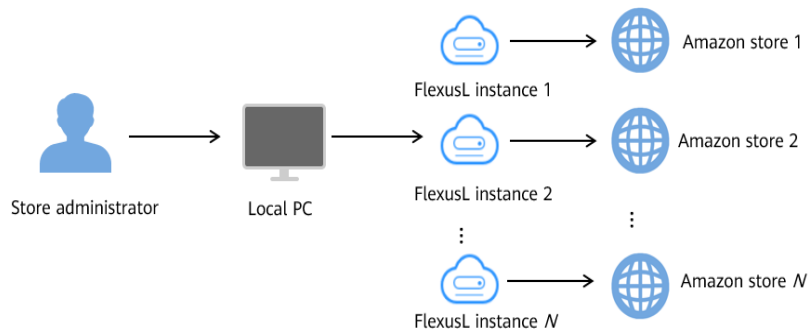
Windows Server is a group of Microsoft-developed OSs for servers. This section uses the Windows Server 2016 OS image as an example to describe how to set up and manage cross-border e-commerce stores. The following uses Amazon stores as an example to show how to manage multiple e-commerce stores on FlexusL instances.

Solution Architecture

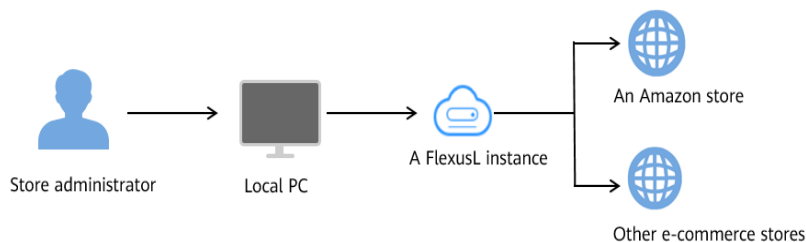
On the Amazon platform, a seller cannot manage multiple accounts from the same public IP address. This can raise red flags and may lead to account suspension or other consequences.



With FlexusL instances, you can log in to different stores from the same host without worrying about account issues.



You can also use the same FlexusL instance to manage stores on other e-commerce platforms.



Resource Planning and Costs

Table 4-5 Resource Planning and Costs

Resource	Type	Description	Cost
Cloud server	<ul style="list-style-type: none"> vCPUs: 2 Memory: 2 GiB 	FlexusL instances are easy to provision and manage. In this example, three FlexusL instances are created, each with 2 vCPUs and 2 GiB memory. You can select proper FlexusL instance flavors based on service requirements. The FlexusL instance names are MyShop_1 , MyShop_2 , and MyShop_3 , respectively.	You need to pay for resources packed in the FlexusL instances. Windows private images are free.
EIP	Automatically assigned	An EIP can be used for Internet access. By default, one fixed EIP is assigned to a FlexusL instance.	
Data disk	10 GiB	Data disks are used to store data except the operating system. They are like drive D, drive E, and drive F in a PC.	
CBR	70 GiB	Cloud Backup and Recovery (CBR) can back up data in system and data disks of FlexusL instances and restore data if instances fail.	
HSS	Host security	Host Security Service (HSS) is designed to improve the overall security of FlexusX instances. It helps you eliminate risks and defend against intrusions and web page tampering. There are also advanced protection and security operations functions available to help you easily detect and handle threats.	
Image	Windows Server 2019	Windows Server 2019 is used.	

Process

Procedure	Description
Preparations	Upload the Windows Server 2019 private image created from the Windows Server 2019 image to the IMS console so that you can select the Windows Server 2019 private image when purchasing FlexusL instances.
Step 1: Purchase FlexusL Instances	Purchase a FlexusL instance and select the Windows Server 2019 private image.
Step 2: Configure Security Groups	Configure inbound rules for a security group to ensure that the FlexusL instance can be accessed.
Step 3: Log In to a FlexusL Instance Server	Set a password and log in to the FlexusL instance server.
Step 4: Remove the Session Time Limit	Set the session time and remove the session time limit to avoid repeated logins due to session timeout.
Step 5: Open Stores	After the preceding steps are complete, you have obtained a complete Windows Server FlexusL instance with a fixed EIP bound. You can create accounts, and open and manage stores on e-commerce websites.

Preparations

To use the Windows Server 2019 image, create a private image from it on the IMS console first.

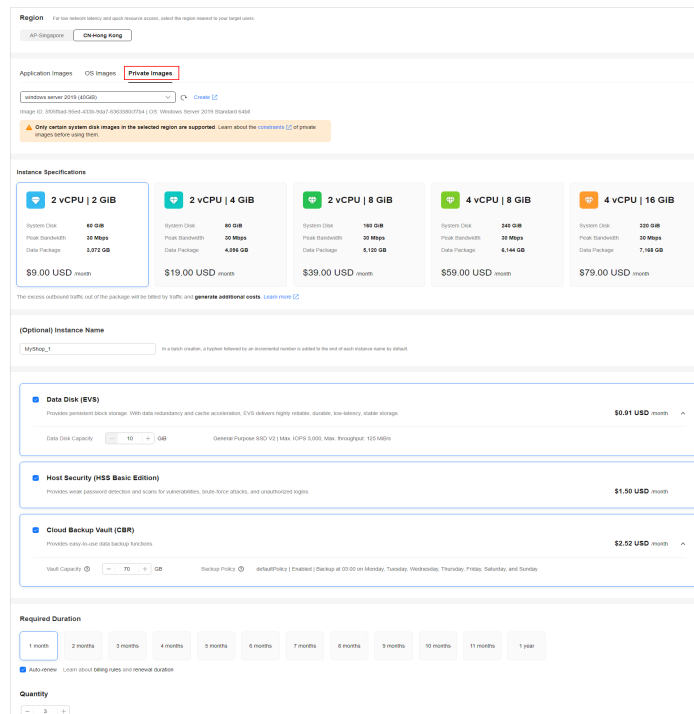
- If your image format is VMDK, VHD, QCOW2, VHDX, QED, VDI, QCOW, or ZVHD, see [Creating a Windows System Disk Image from an External Image File](#).
- If your image format is ISO, see [Creating a Windows System Disk Image from an ISO File](#).
- If your image format is RAW or ZVHD2, see [Quickly Importing an Image File](#).

NOTICE

Images are regional resources. FlexusL instances only can use private images that are in the same region as them. Ensure that the image is in the same region as the FlexusL instance.

Step 1: Purchase FlexusL Instances

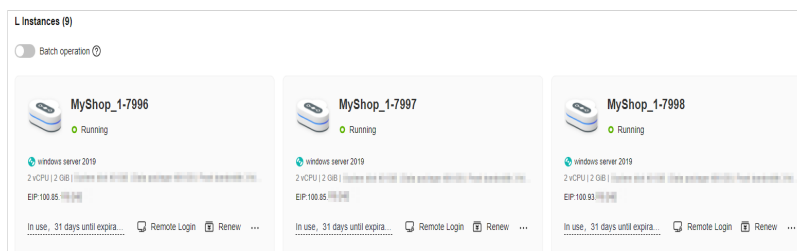
1. Log in to the FlexusL [console](#) and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Image	Windows Server 2019	In the private image list, select the Windows Server 2019 private image which is in the same region (CN-Hong Kong) as the instance and has been uploaded to the IMS console.
Instance Specifications	2 vCPUs 2 GiB memory and 60 GiB system disk	Select instance specifications as required.
Instance Name	MyShop_1	Customize an instance name that is easy to identify, for example, MyShop_1, MyShop_2, and MyShop_3.

Parameter	Example	Description
(Optional) Associated Services	<ul style="list-style-type: none"> Data Disk: 10 GiB Host Security Cloud backup vault: 70 GiB 	You can bundle any of the services to your FlexusL instances as needed: EVS, HSS (basic edition), and CBR.
Required Duration	<ul style="list-style-type: none"> 1 month Enabling auto-renew 	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	3	Set the number of FlexusL instances to be purchased, for example, three in this example.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

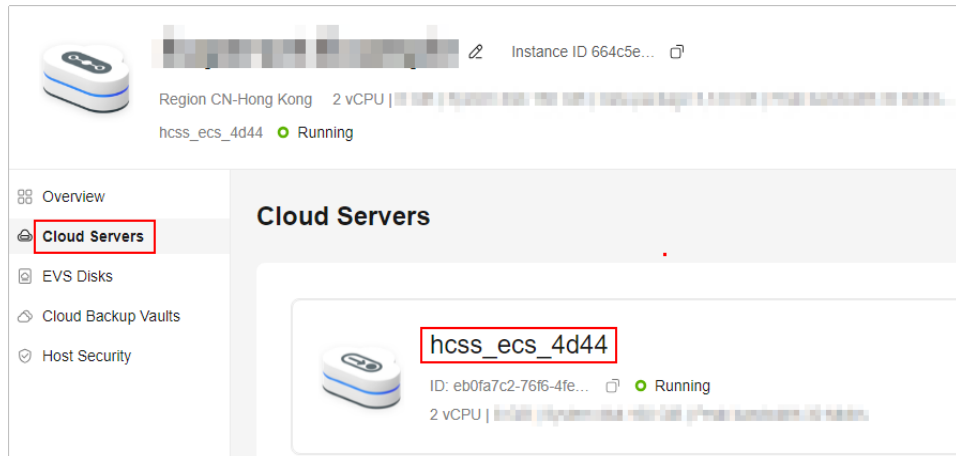


5. Hover the pointer over a resource card, click  next to the instance name, and change it to **MyShop_1**, **MyShop_2**, and **MyShop_3**, respectively.

Step 2: Configure Security Groups

Configure inbound rules for security groups to ensure that the FlexusL instance can be accessed.

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.

The following figure only displays common rules. You can add more rules as needed.

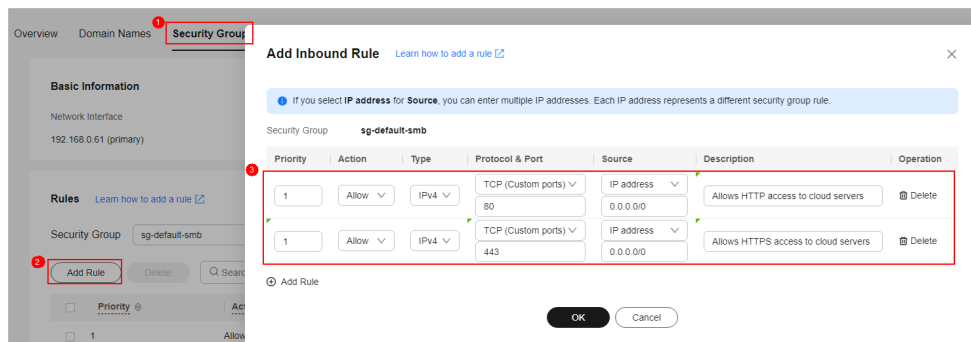


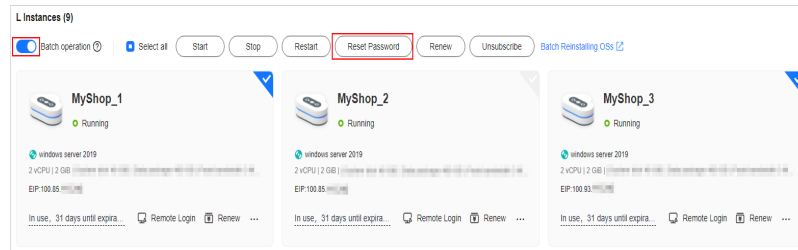
Table 4-6 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Allows HTTP traffic to FlexusL instances.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS traffic to FlexusL instances.

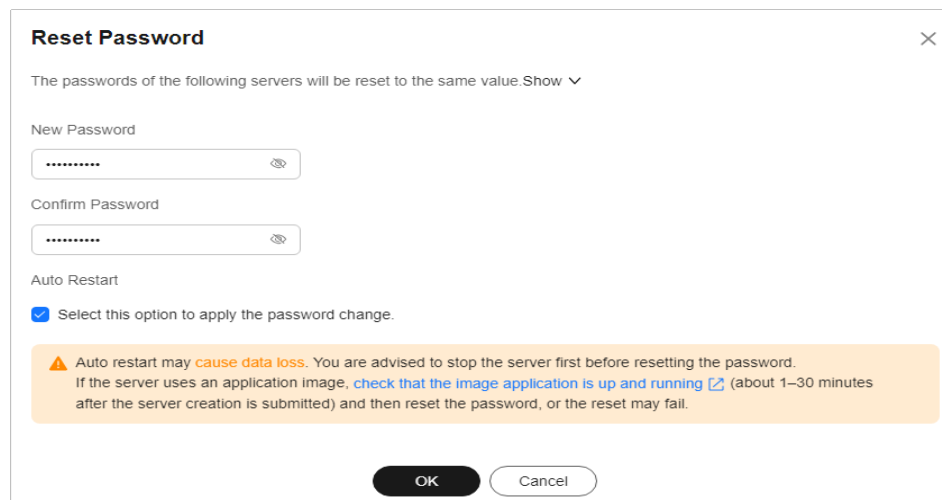
Step 3: Log In to a FlexusL Instance Server

For Windows FlexusL instances, the administrator username is **Administrator** and there is no default password. Set a password before logging in to the server.

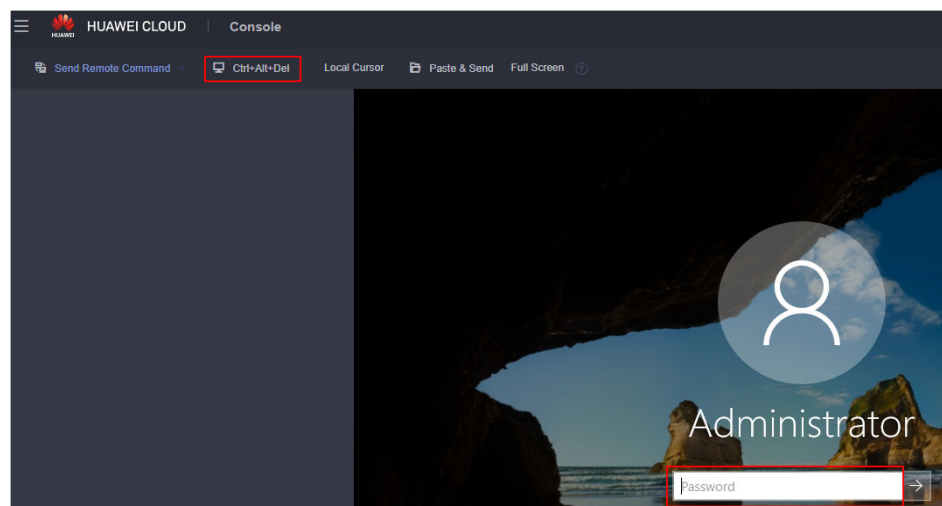
1. Enable **Batch operation**, select **Select all**, and click **Reset Password**.



2. Set a new password for the FlexusL instance servers and click **OK**.
If you reset the password for running servers, the password change is applied only after the next restart. Select **Auto Restart**. After the password is reset, the server status becomes **Restarting**. Wait until the status changes to **Running** and go to the next step.



3. In the resource card, click **Remote Login** to remotely log in to the cloud server using VNC.
4. Click **Ctrl+Alt+Del** in the upper left corner to unlock the desktop. Follow the instructions to enter the password set in step 2 and press **Enter**.

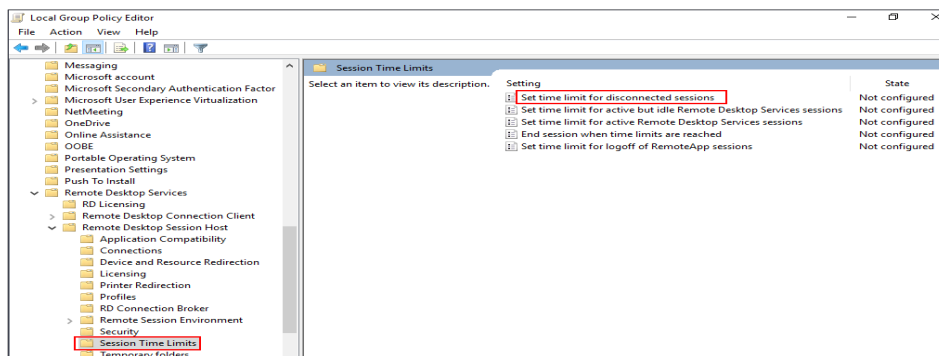


Step 4: Remove the Session Time Limit

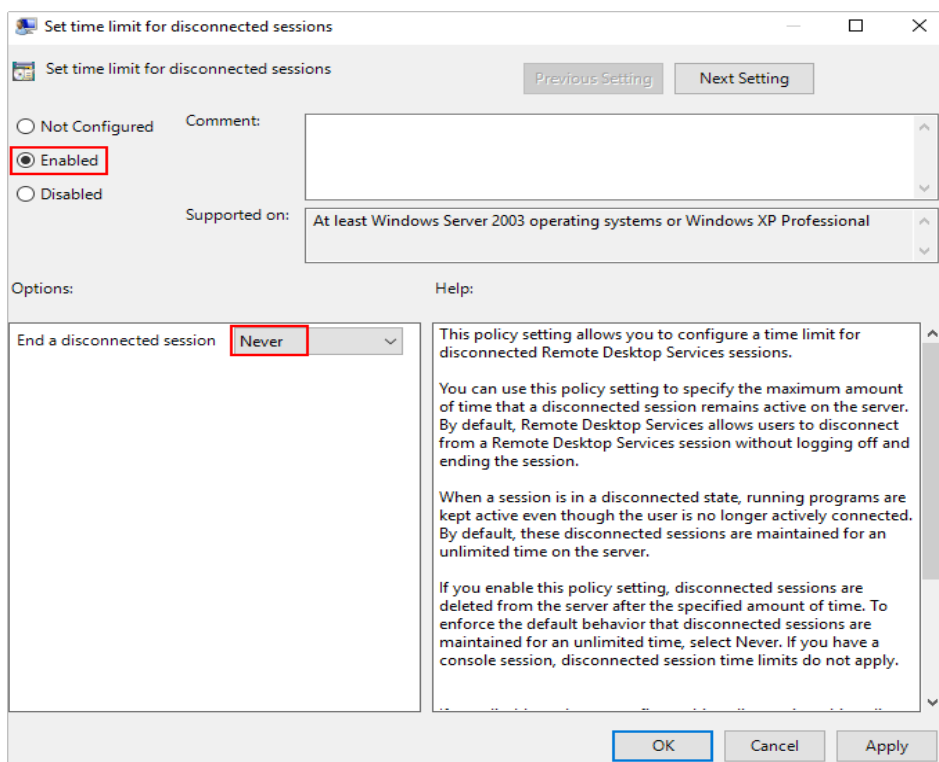
A session is a sequence of uninterrupted requests and responses between a user and a server. Session timeout occurs when a user does not perform any action

within a specified period and the session of the user is terminated. Once the session times out, you need to log in to the FlexusL instance server again. This section describes how to remove the session time limit.

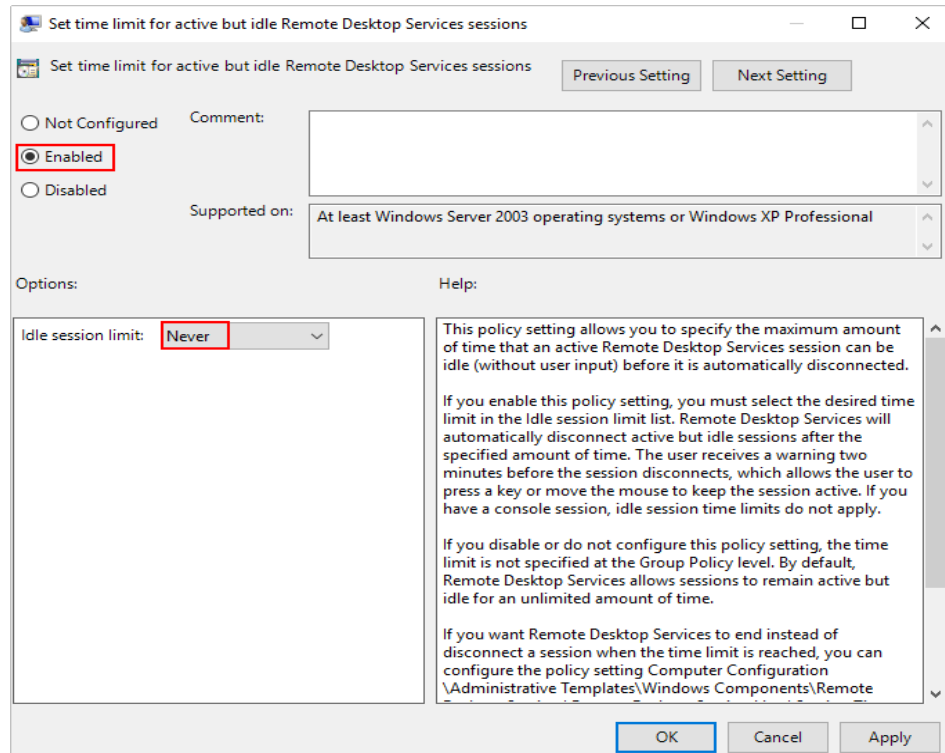
1. In the search box at the lower left corner of the page, search for **RUN**.
2. Enter **gpedit.msc** in the **RUN** dialog box and click **OK**.
3. In the **Local Group Policy Editor** window, choose **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Session Time Limits**, and double-click **Set time limit for disconnected sessions** in the right pane.



4. In the displayed dialog box, select **Enabled** and set **End a disconnected session** to **Never**. Click **OK**.



5. In the **Local Group Policy Editor** window, double-click **Set time limit for active but idle Remote Desktop Services sessions** in the right pane.
6. In the displayed dialog box, select **Enabled** and set **Idle session limit** to **Never**. Click **OK**.



Step 5: Open Stores

Now you have obtained a Windows Server FlexusL instance with a fixed EIP bound. You can create accounts, and open and manage stores on e-commerce websites.

When running e-commerce stores, you may need to upload your local files to cloud servers. For details, see [How Do I Upload Files to My ECS](#) (The method also applies to uploading files to FlexusL instances).

4.3.2 Using PrestaShop to Build an E-Commerce Website

Application Scenario

PrestaShop is a full-featured, cross-platform, and open source e-commerce platform written in the PHP programming language with support for the MySQL database management system. PrestaShop supports transactions using different currencies and almost all payment methods, such as Paypal. It is a good choice for you to build foreign trade websites. Supported By FlexusL, the PrestaShop application image uses Ubuntu 22.04 and is deployed using Docker. The Nginx, MySQL, phpMyAdmin, and Docker have been preconfigured in the image. This section describes how to use PrestaShop to build an e-commerce website.

Resource Planning and Costs

This practice uses the following resource planning as an example. You can adjust it as required.

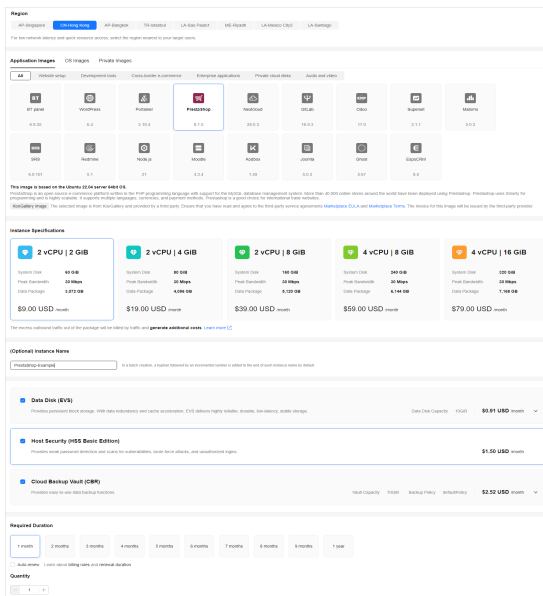
Resource	Configuration	Description
Cloud server	<ul style="list-style-type: none"> vCPUs: 2 Memory: 2 GiB 	Select appropriate instance specifications based on your service requirements.
Image	PrestaShop	Select the PrestaShop application image.
Security group	Inbound rule: <ul style="list-style-type: none"> Protocol/ Application: TCP Port: 9001, 9000, 3306 Source: 0.0.0.0/0 	<ul style="list-style-type: none"> 80: Specifies the internal forwarding port of application images. 9000: Allows external access to the application O&M page. 9001: Allows external access to the application management page. 3306: Allows access to MySQL databases.
Domain name	wpwebsite.com	<ul style="list-style-type: none"> If the website is only used for personal development or testing, there is no need to add a domain name. If the website is open to the public, add and resolve a domain name for the cloud server.

Procedure

Procedure	Description
Step 1: Purchase a FlexusL Instance	Purchase a FlexusL instance and select the PrestaShop application image.
Step 2: Configure Security Groups	Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.
Step 3: Reset the Password and Log In to the FlexusL Instance	A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance.
Step 4: Initialize Prestashop	Log in to PrestaShop and select the desired language for the management page.
Step 5: Deploy Prestashop	On the dashboard, perform the following operations: <ul style="list-style-type: none"> Manage language packages and set languages Manage modules Back up databases Configure domain names

Step 1: Purchase a FlexusL Instance

1. Log in to the FlexusL [console](#) and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Application Image	PrestaShop	Select the PrestaShop application image.
Instance Specifications	2 vCPUs 2 GiB System disk 60 GiB	Select instance specifications as needed.
Instance Name	PrestaShop-Example	Customize an instance name that is easy to identify, for example, PrestaShop-Example.
(Optional) Associate Services	<ul style="list-style-type: none"> • Data Disk: 10 GiB • Host Security • Cloud backup vault: 70 GiB 	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.

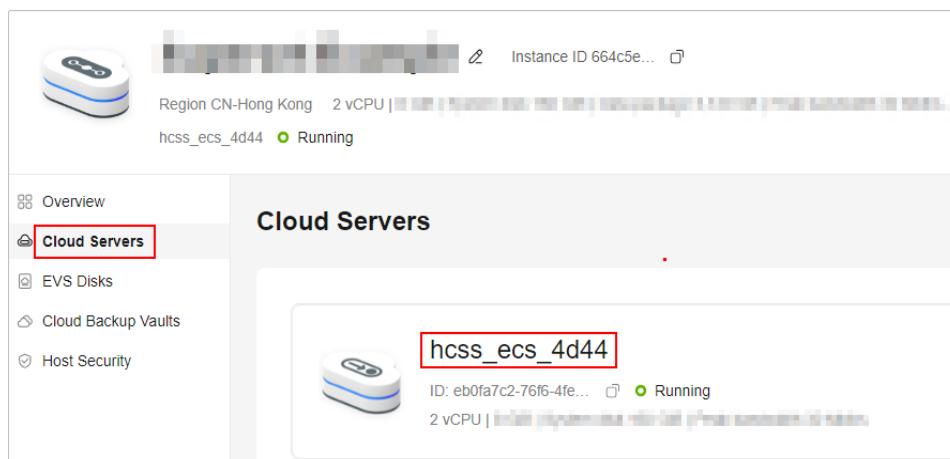
Parameter	Example	Description
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure Security Groups

Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.
The following figure only displays common rules. You can add more rules as needed.

Table 4-7 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of application images
1	Allow	IPv4	TCP: 3306	0.0.0.0/0	Allows access to MySQL databases.
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M page.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

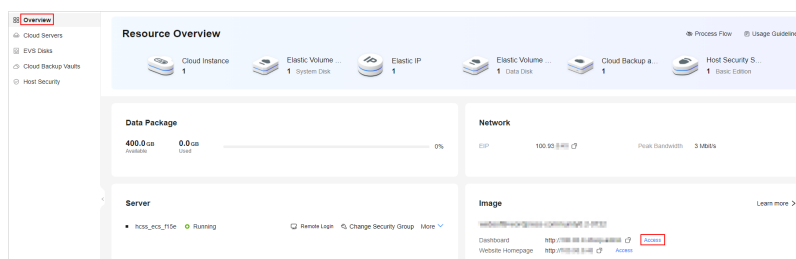
Step 3: Reset a Password

A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance. The password of the FlexusL instance is also used for [logging in to the O&M page of the application](#).

1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard and check whether the application has been up and running. If yes, go to the next step.

NOTICE

Wait for several minutes until the image with the pre-installed application is up and running. Then, you can perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the initial password may become invalid and you cannot log in to the application dashboard.

Figure 4-10 Entry to the application dashboard

NOTICE

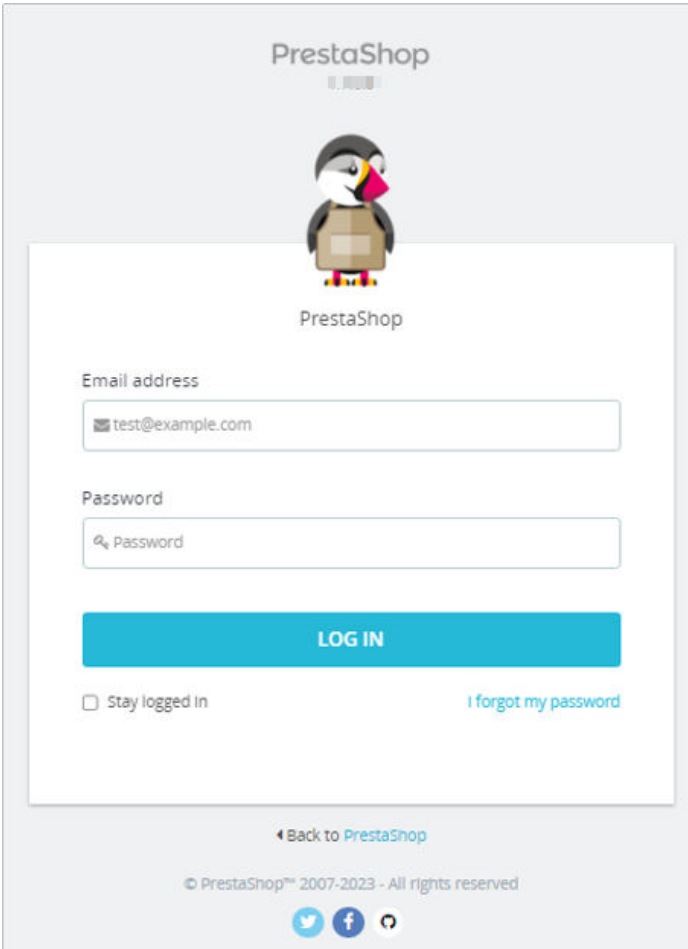
When you click **Access** to go to the dashboard for the **first time**, PrestaShop generates a random character string following the dashboard address for encryption. **Keep the encrypted dashboard address in mind. You can only use the encrypted address to log in to the dashboard and cannot access the dashboard from the console.**

For example, when you access the management console `http://1.1.1.1:9001/admin` for the first time, the address automatically changes to `http://1.1.1.1:9001/admin923reep1k/index.....`, where the character string **923reep1k** is added after **admin**. Keep the address `http://1.1.1.1:9001/admin923reep1k` in mind. (You do not need to record the part following **admin923reep1k/**)

You can also reinstall the FlexusL instance to obtain the new dashboard address, but the original data will be lost. Therefore, keep the encrypted address in mind.

After the application is started, the initialization wizard page of the dashboard is displayed, as shown in [Figure 4-11](#).

Figure 4-11 Initialization wizard page of the Prestashop dashboard



PrestaShop

PrestaShop

Email address

test@example.com

Password

Password

LOG IN

Stay logged in [i forgot my password](#)

[Back to PrestaShop](#)

© PrestaShop™ 2007-2023 - All rights reserved

NOTE

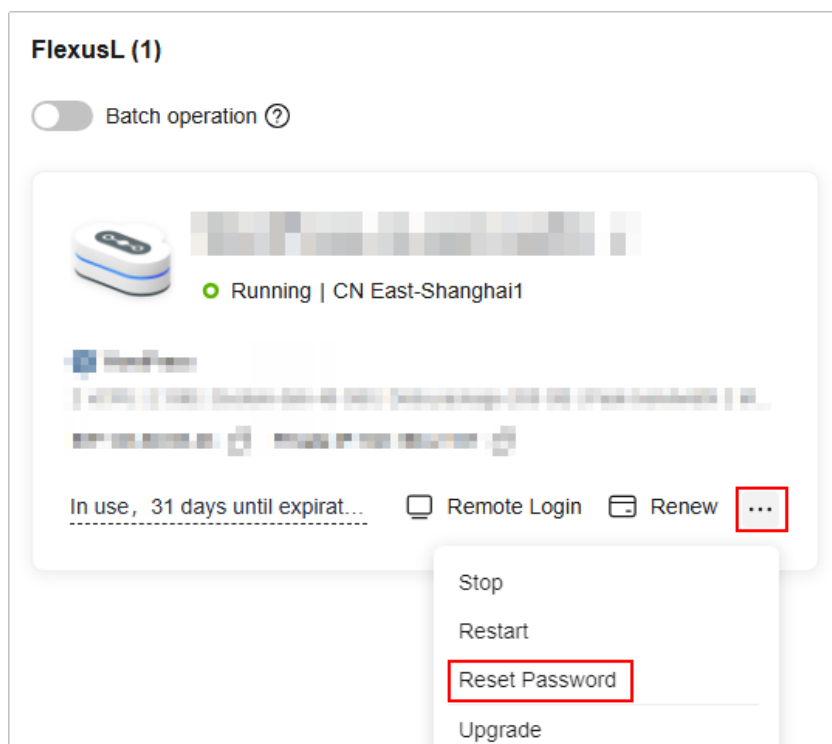
If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
- The dashboard is being started. Try again later.

2. Locate the resource card and choose **...** > **Reset Password** to reset the password.

For details, see [Resetting the Password for a FlexusL Instance](#).

Figure 4-12 Resetting a password

**NOTE**

The password for logging in to the FlexusL instance is also the password for logging in to the O&M page of the application.

Step 4: Initialize Prestashop

Application images use code-based Ubuntu. They provide graphical user interfaces to make your operations easier. You need to initialize the application dashboard upon the first login. Then you can directly log in to the dashboard from the FlexusL console afterwards.

1. In the address bar of a local browser, enter **http://<Server-EIP>:9000** to log in to the application O&M page.

The initial username and password for logging in to the application dashboard are stored on the O&M page of the application. You need to log in to the O&M page first to obtain the username and password. The username

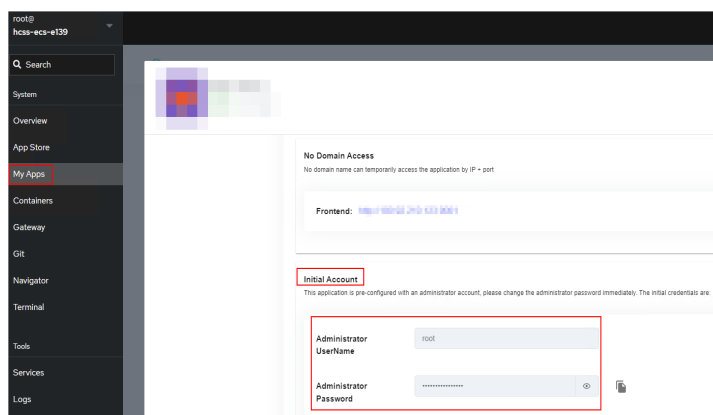
for logging in to the O&M page is **root**, and the login password is the password reset in 2.

NOTE

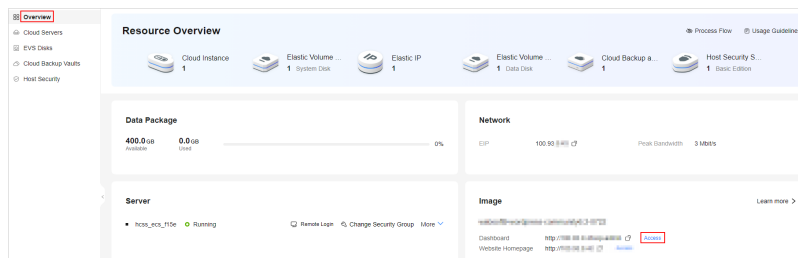
For details about the FlexusL instances, O&M page, and dashboard, see [What Is the Relationship Among FlexusL Instances, the Dashboard, and the O&M Page?](#)

2. On the **My Apps** page, click the application icon, choose **Access**, and click **Initial Account** to view the username and password for logging in to the application management page.

The initial password is a randomly generated strong password. After the application is initialized, change the password on the dashboard for easy management. If the password is changed, the initial password will be invalid. Remember the new password.



3. On the **Overview** page, click **Access** in the **Dashboard** field in the **Image** area.



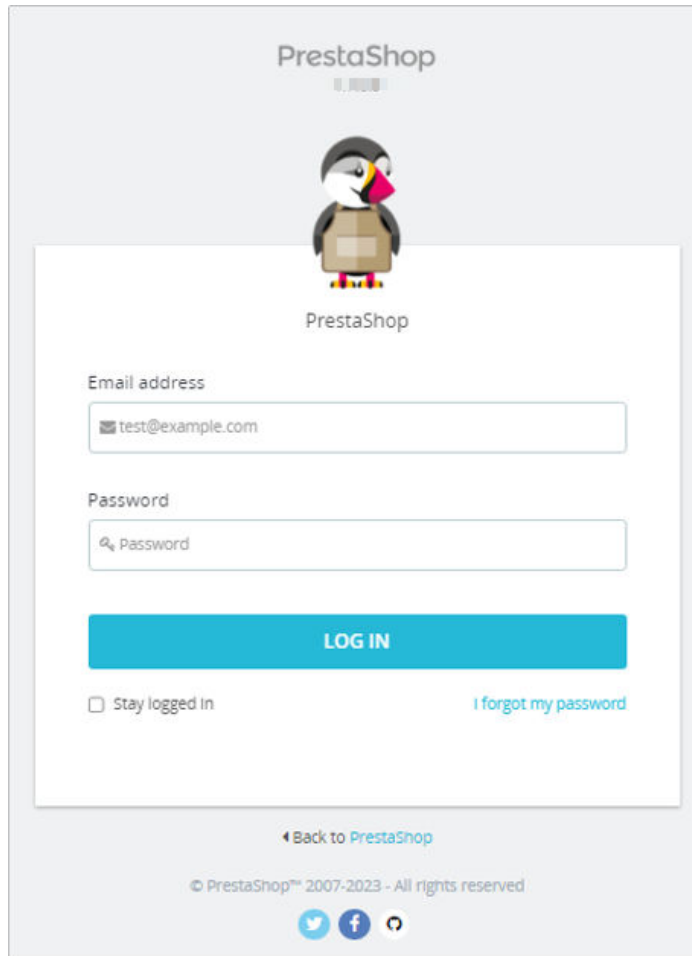
NOTE

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
- The dashboard is being started. Try again later.

4. Enter the password obtained in 2.

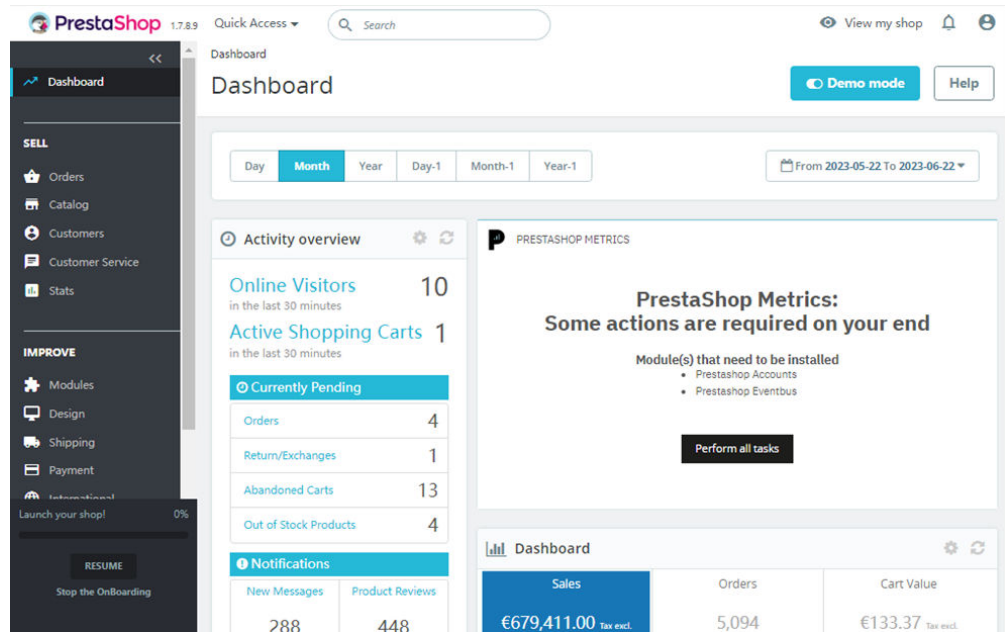
Figure 4-13 Initialization wizard page of the Prestashop dashboard



NOTE

If a message is displayed indicating that the username or password you entered is invalid when you attempt to log in to the application dashboard, refer to [Why Can't I Access the Dashboard of the Application Pre-installed in the Application Image After Entering the Initial Username and Password?](#)

5. Click **LOG IN** to log in to PrestaShop.



After the Prestashop application is initialized, you can deploy your applications on the dashboard.

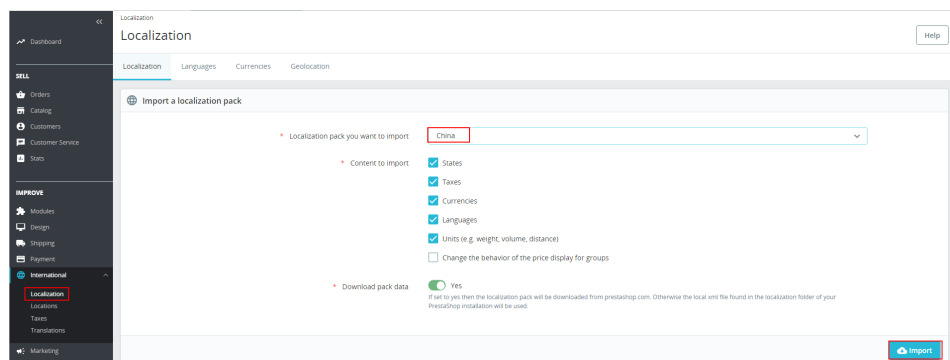
Step 5: Deploy Prestashop

This section describes some basic operations of PrestaShop. For more information, see [PrestaShop Documentation](#).

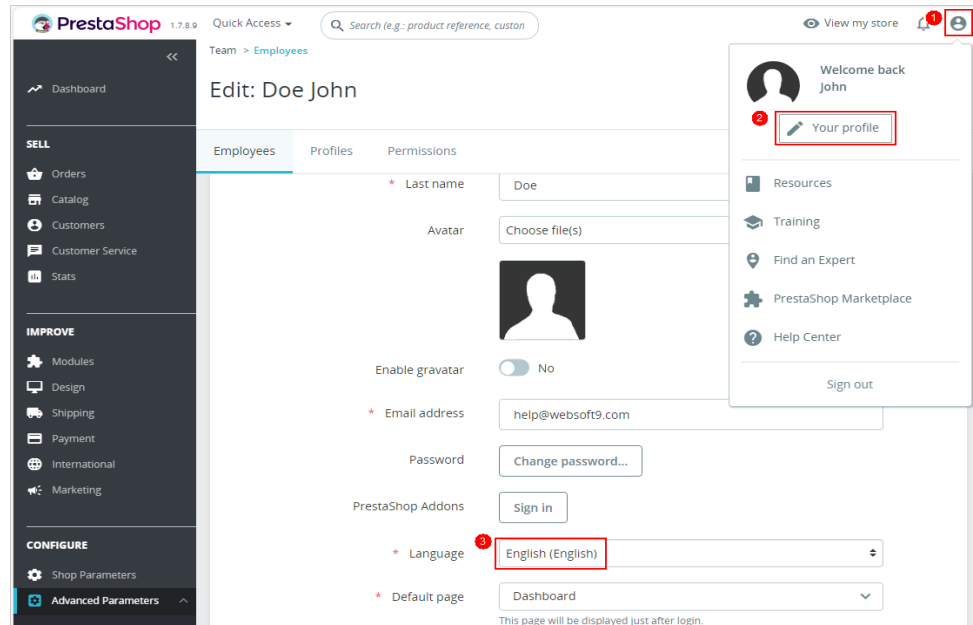
Managing Language Packages

PrestaShop has a built-in multi-language system. You only need to select the corresponding language and import it to your PrestaShop system online.

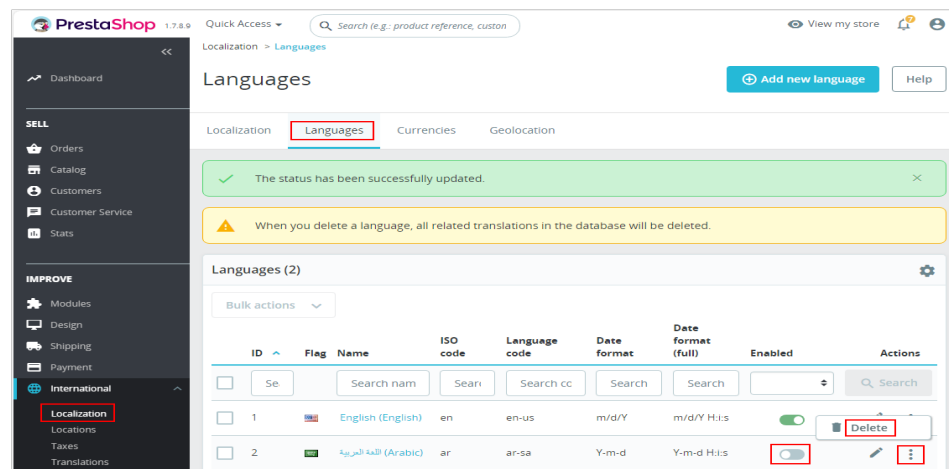
- Import a language package.
 - a. Choose **IMPROVE > International > Localization**, select the language package you want to import, and click **Import**.



- b. Click the **Languages** tab to view the language packages that have been imported.
- Set the language of the dashboard.
Click the avatar on the right corner, select **Your profile** and set the language. Click **Save**.



- Delete a language package.
You can delete unnecessary language packages.
- a. Choose **International > Localization > Languages** and disable the language package you want to delete.



- b. In the **Actions** list, click **Delete** to delete the language that is disabled.

Managing Modules

PrestaShop has a rich module library, which greatly expands the functions of PrestaShop.

- Choose **Modules > Marketplace**, find the required plug-in, and click **Buy Now** or **Install** to purchase and install the module.
You can also click **Upload a module** to install other modules.
- Choose **Modules > Module Manager**.
 - On the **Modules** tab page, you can disable, configure, uninstall, and restore the modules.

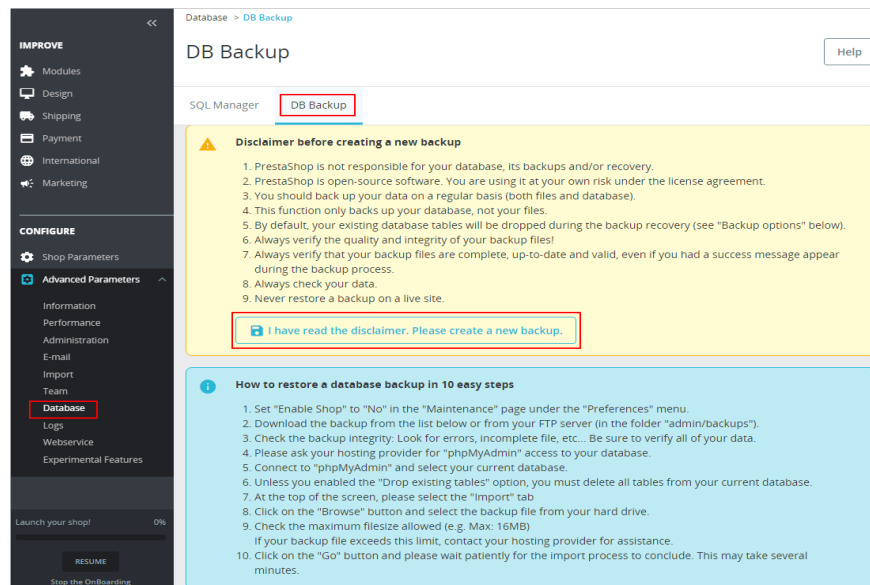
- On the **Alerts** tab page, you can view the notifications of modules.
- On the **Updates** tab page, you can view modules that can be updated.

Backing Up Databases

PrestaShop allows you to back up databases.

1. In the navigation pane on the left, choose **Advanced Parameters > Database > DB Backup**, read the disclaimer, and click **I have read the disclaimer. Please create a new backup.**

You can follow the instructions on the following page to restore a database.



2. Click **Download the backup file** to download the backup file to your local PC.

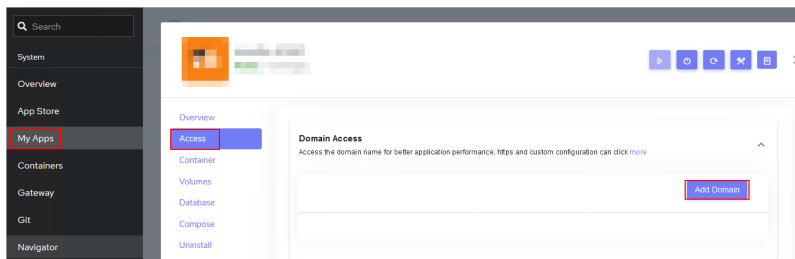
Configuring Domain Names

Add and resolve a domain name for the website so that users can use the domain name to access the website. If the website is only used for personal development or testing, there is no need to add a domain name.

1. If the domain name is not registered with Huawei Cloud or not hosted on Huawei Cloud DNS, the domain name cannot be resolved. Use either of the following methods to resolve the issue:
 - Contact the DNS service provider to add an A record that maps the domain name to the EIP of the FlexusL instance.
 - Use Huawei Cloud DNS servers to resolve the domain name. For details, see [Migrating to Huawei Cloud DNS for Domain Name Resolution](#).
2. Add the domain name on the application O&M page.
 - a. In the address bar of a local browser, enter **http://EIP:9000** to log in to the application O&M page.

The username and password for logging in to the dashboard are the **root** user and password of the FlexusL instance. A FlexusL instance does not have an initial password. Reset the password and use it to log in to the dashboard.

- b. Choose **My Apps** and click the App icon.
- c. Choose **Access** and click **Add Domain**.



3. Apply for ICP licensing for the domain name.

To successfully access the server using a domain name, you must license the domain name. Domain name licensing provided by the ICP License Service is free of charge. For details, see [ICP Filing Process](#).

After the domain name is licensed, you can use it to visit the website.

4.4 Audio and Video Scenarios

4.4.1 Pushing Local PC Desktop Streams to SRS Using OBS

Application Scenario

SRS is a simple and an efficient real-time video server that supports various real-time streaming media protocols, such as RTMP, WebRTC, HLS, HTTP-FLV, and SRT. Supported By FlexusL, the SRS image uses Ubuntu 22.04 and is deployed using Docker. The Nginx and Docker have been preconfigured in the image. This section describes how to push PC desktop streams to SRS using OBS.

Resource Planning and Costs

This practice uses the following resource planning as an example. You can adjust it as required.

Resource	Configuration	Description
Cloud server	<ul style="list-style-type: none">vCPUs: 2Memory: 4 GiB	Select appropriate instance specifications based on your service requirements.
Image	SRS	Select the SRS application image.

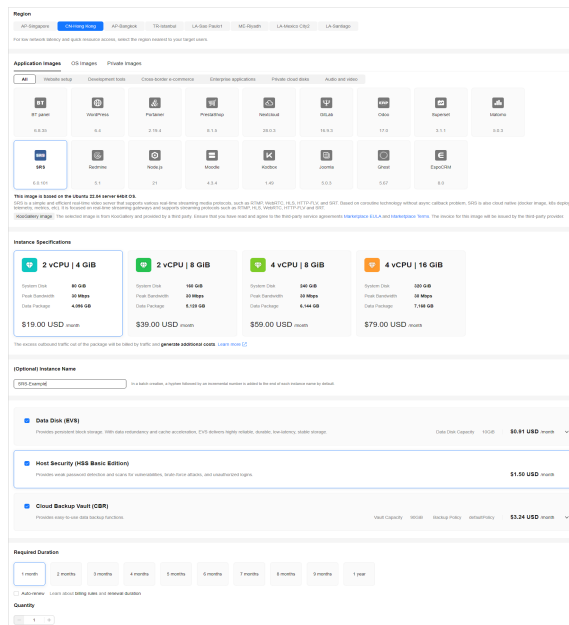
Resource	Configuration	Description
Security group	Inbound rule: <ul style="list-style-type: none"> Protocol & Port TCP: 80, 9001, 1935, 1985, 8080, 8000 Source: 0.0.0.0/0 Protocol & Port ICMP: all Source: 0.0.0.0/0 	<ul style="list-style-type: none"> 80: Specifies the internal forwarding port of application images. 9001: Allows external access to the application management page. 1935: Allows access to the RTMP livestreaming server. 1985: Allows access to the HTTP API server to deliver HTTP-API and WebRTC streams. 8080: Allows access to the HTTP livestreaming server to deliver HTTP-FLV and HLS streams. 8000: Allows access to the WebRTC media server.
Domain name	wpwebsite.com	<ul style="list-style-type: none"> If the website is only used for personal development or testing, there is no need to add a domain name. If the website is open to the public, add and resolve a domain name for the cloud server.

Process

Procedure	Description
Step 1: Purchase a FlexusL Instance	Purchase a FlexusL instance and select the SRS application image.
Step 2: Configure Security Groups	Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.
Step 3: Reset the Password and Log In to the FlexusL Instance	A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance before logging in to it.
Step 4: Learn About the SRS Dashboard	Understand the SRS working interface.
Step 4: Push Local PC Desktop Streams to SRS Using OBS	Learn how to push local PC desktop streams to SRS using OBS.

Step 1: Purchase a FlexusL Instance

1. Log in to the FlexusL [console](#) and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Application Image	SRS	Select the SRS application image.
Instance Specifications	2 vCPUs 4 GiB memory and 80 GiB system disk	Select instance specifications as needed.
Instance Name	SRS-Example	Customize an instance name that is easy to identify, for example, SRS-Example.

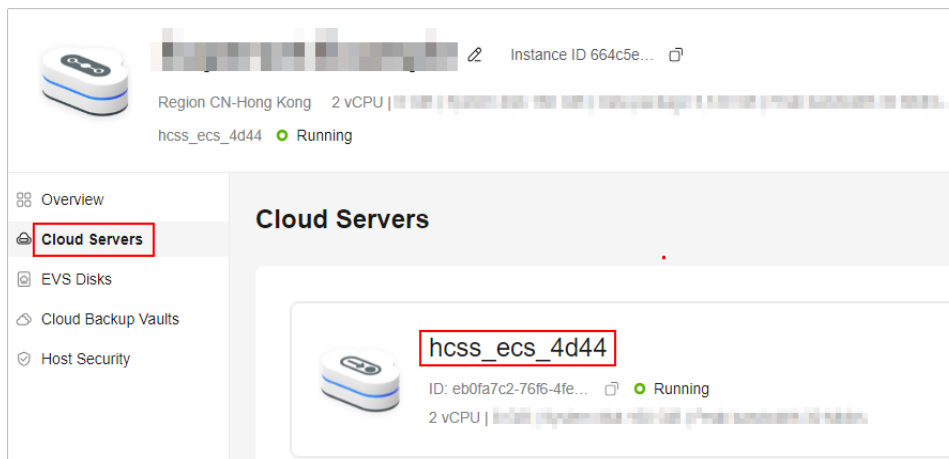
Parameter	Example	Description
(Optional) Associated Services	<ul style="list-style-type: none">• Data disk: 10 GiB• Host security• Cloud backup vault: 90 GiB	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure Security Groups

Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.

The following figure only displays common rules. You can add more rules as needed.

Table 4-8 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
100	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.
100	Allow	IPv4	TCP: 1935	0.0.0.0/0	Allows access to the RTMP livestreaming server.
100	Allow	IPv4	TCP: 1985	0.0.0.0/0	Allows access to the HTTP API server to deliver HTTP-API and WebRTC streams.
100	Allow	IPv4	TCP: 8080	0.0.0.0/0	Allows access to the HTTP livestreaming server to deliver HTTP-FLV and HLS streams.
100	Allow	IPv4	TCP: 8000	0.0.0.0/0	Allows access to the WebRTC media server.

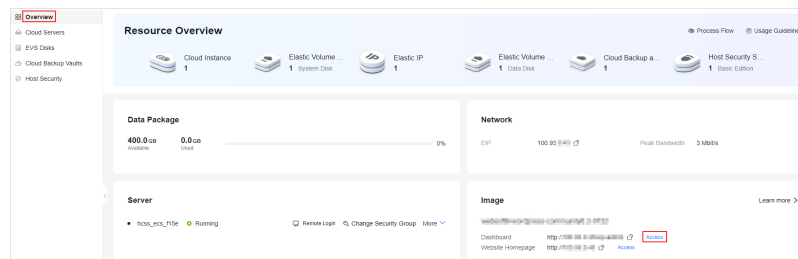
Step 3: Reset the Password and Log In to the FlexusL Instance

This section describes how to log in to a FlexusL instance. A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance before logging in to it.

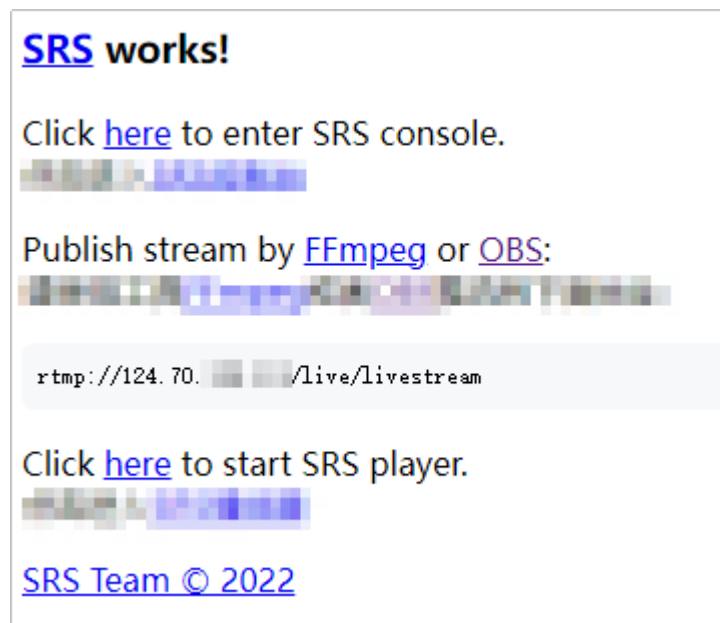
1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard and check whether the application has been up and running. If yes, go to the next step.

NOTICE

Wait for several minutes until the image with the pre-installed application is up and running. Then, you can perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the initial password may become invalid and you cannot log in to the application dashboard.

Figure 4-14 Entry to the application dashboard

After the application is started, the initialization wizard page of the dashboard is displayed, as shown in [Figure 4-15](#).

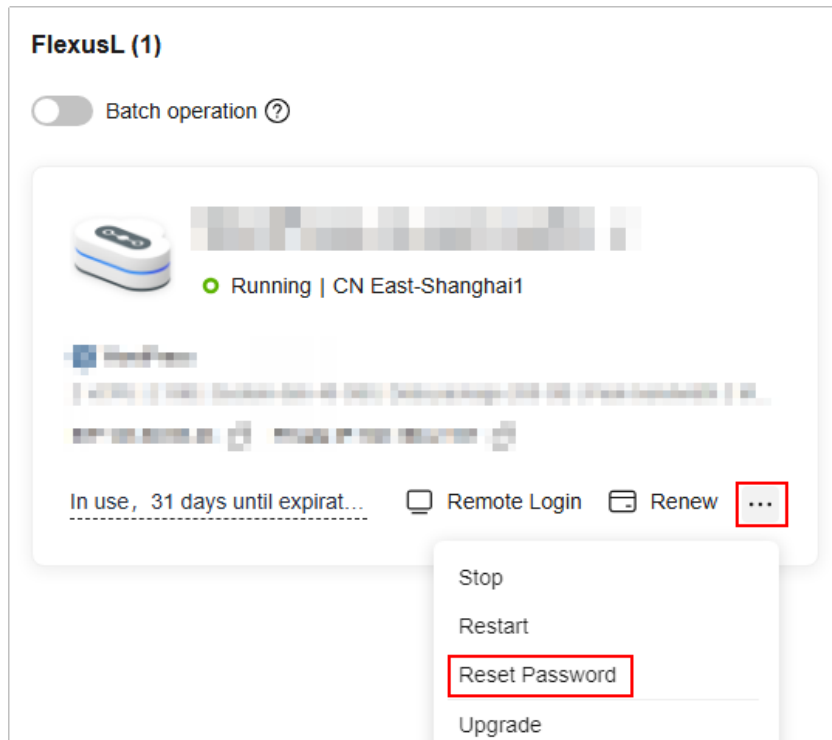
Figure 4-15 Initial page of the SRS dashboard**NOTE**

If the dashboard is not properly displayed, check the following causes:

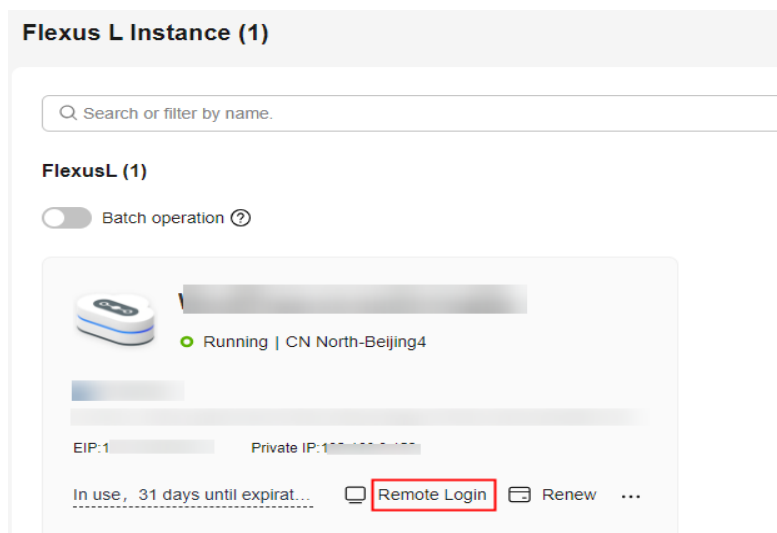
- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
 - The dashboard is being started. Try again later.
2. Locate the resource card and choose **...** > **Reset Password** to reset the password.

A FlexusL instance does not have an initial password. Set a password for the FlexusL instance before logging in to it. For details, see [Resetting the Password for a FlexusL Instance](#).

Figure 4-16 Resetting a password



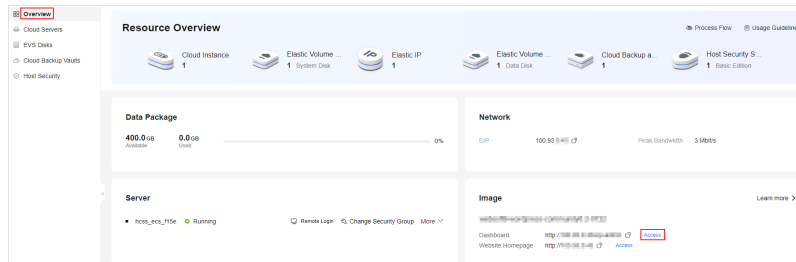
3. Locate the target instance and click **Remote Login** and enter the username and password as prompted to log in to the FlexusL instance. The username is **root**, and the password is the one set in 2.



Step 4: Learn About the SRS Dashboard

Application images are based on the Ubuntu OS of the code page. You can log in to the **visualized dashboard** to configure applications easily.

1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard.

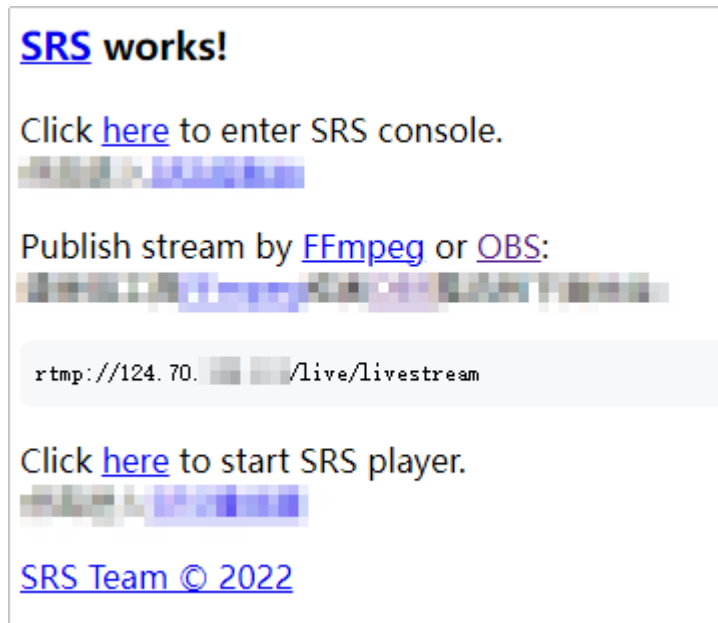


NOTE

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
 - The dashboard is being started. Try again later.
2. Check the SRS dashboard.
You do not need to set the username and password for logging in to SRS. On the SRS dashboard, you can:
 - Log in to the SRS console.
 - Obtain the ingest URL.
 - Start SRS player to watch the livestreaming content.

Figure 4-17 Initial page of the SRS dashboard



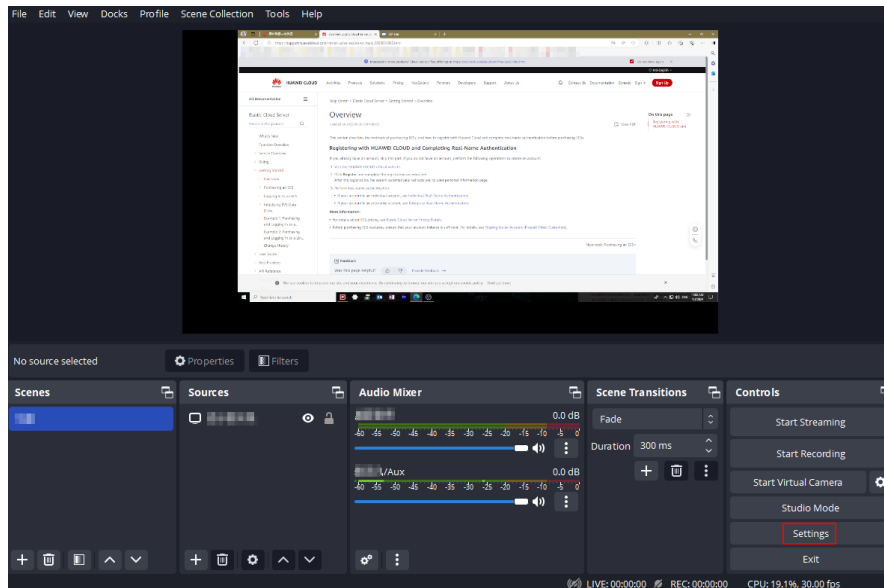
After the SRS application is set up, you can use SRS to push and watch livestreams.

Step 4: Push Local PC Desktop Streams to SRS Using OBS

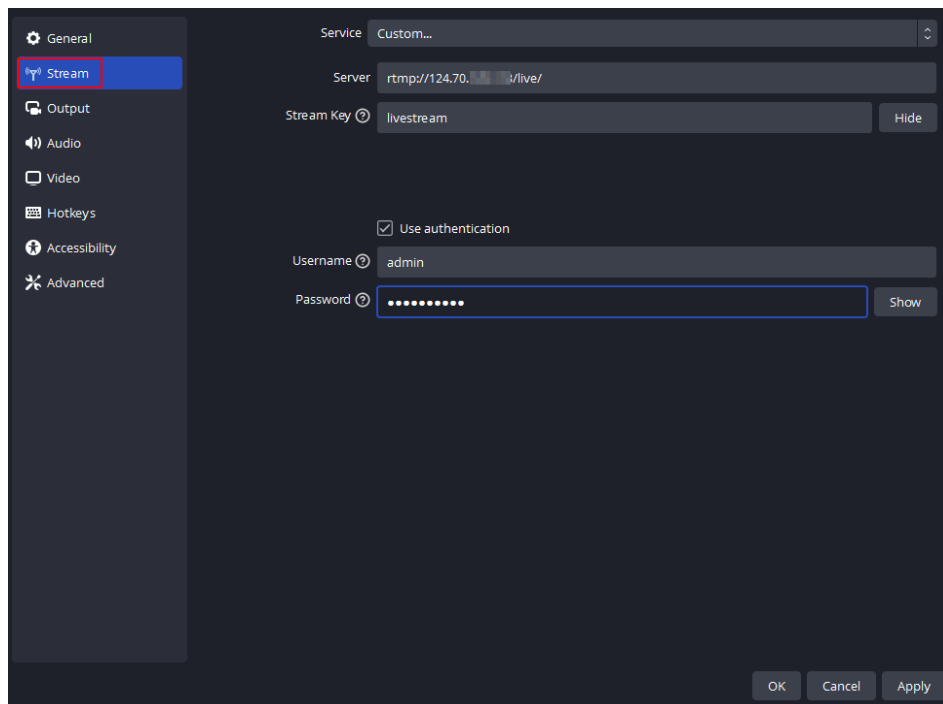
This section describes how to push local PC desktop streams to SRS using OBS.

Step 1: Push Livestreams

1. **Download** and install OBS based on your operating system.
2. Open OBS tool and click **Settings** in the **Controls** area.

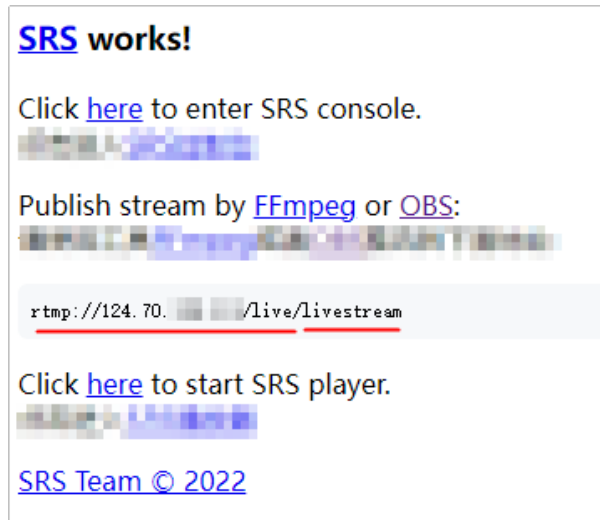


3. On the **Stream** page, configure parameters and click **Apply**.

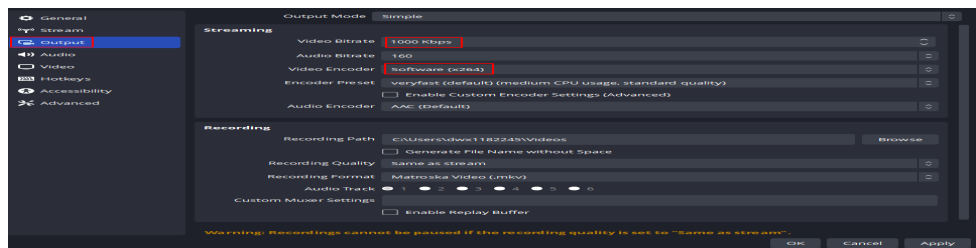


Parameter	Description
Service	Multiple platforms can push livestreams via OBS. For SRS, select Custom .
Server	Enter the stream pushing address specified by SRS, for example, rtmp://124.70.x.x/live/ .

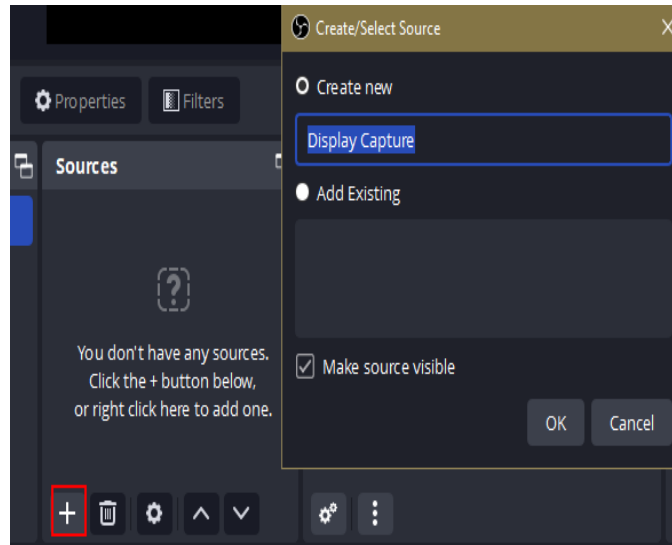
Parameter	Description
Stream key	Specify a character string following the specified stream pushing address, for example, the livestream following live/ in rtmp://124.70.x.x/live/ .
Use authentication	Select Use authentication and set the Username and Password .



- In the **Output** page, configure parameters and click **Apply**. Set **Video Bitrate** to **1000 kbps**. Select **Software** for **Video Encoder** to avoid the need for high-end graphics cards and prevent potential streaming issues. Configure other parameters as needed.



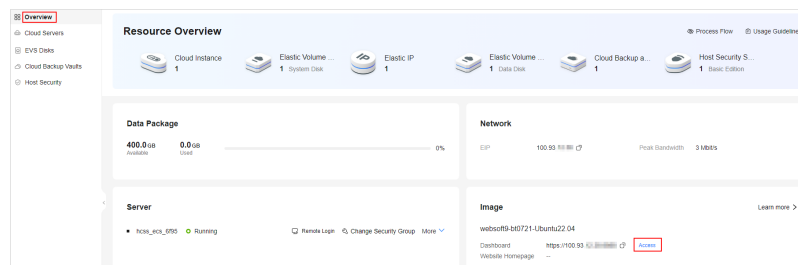
- Click **OK**.
- In the displayed **Sources** area, click **+**, select **Display Capture**, create a source, and click **OK**.



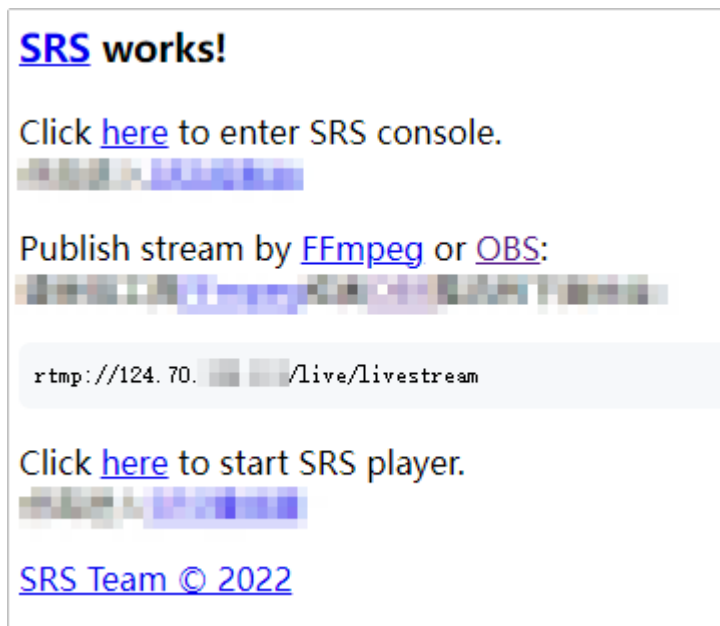
7. Perform any operation to change the desktop screen, and you can see that the screen starts to capture desktop content. Click **OK**.
8. Click **Start Streaming**. After the connection is successful, a green block is displayed in the lower right corner, indicating that the stream pushing is successful.

Step 2: Watch Livestreams

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.
2. On the **Overview** page, in the **Image** area, click **Access** to access the image application dashboard.



3. Start SRS player.



4. Watch the desktop livestreams.

4.5 Website Data Analysis

4.5.1 Using Superset to Obtain Data from MySQL for Analysis

Application Scenario

Superset is an open-source data exploration and visualization platform. This tool provides a quick way to intuitively visualize datasets by allowing you to create and share interactive dashboards. Supported By FlexusL, the Superset application image uses Ubuntu 22.04 and is deployed using Docker. The Nginx, Redis, pgAdmin, and Docker have been preconfigured in the image. This section describes how to use Superset to obtain data from MySQL databases for analysis.

Resource Planning and Costs

This practice uses the following resource planning as an example. You can adjust it as required.

Resource	Configuration	Description
Cloud server	vCPUs: 2 Memory: 8 GiB	A Superset application image requires at least 2 vCPUs and 8 GiB of memory. Select appropriate instance specifications accordingly.
Image	Superset	Select the Superset application image.

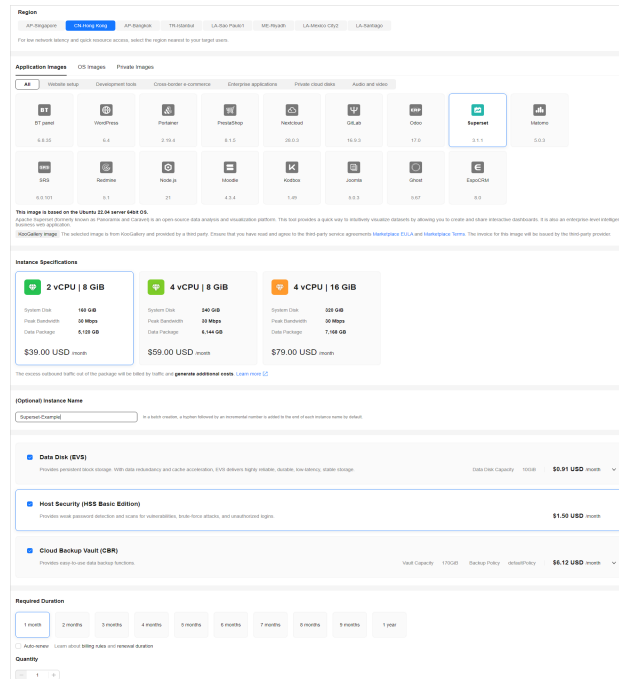
Resource	Configuration	Description
Security group	Inbound rule: <ul style="list-style-type: none">• Protocol/ Application: TCP• Port: 80, 9000, 9001, 3306• Source: 0.0.0.0/0	<ul style="list-style-type: none">• 80: Specifies the internal forwarding port of application images.• 9000: Allows external access to the application O&M page.• 9001: Allows external access to the application management page.• 3306: Allows access to MySQL databases.

Procedure

Procedure	Description
Step 1: Purchase a FlexusL Instance	Purchase a FlexusL instance and select the Superset application image.
Step 2: Configure Security Groups	Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.
Step 3: Reset the Password and Log In to the FlexusL Instance	A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance.
Step 4: Initialize Superset	Set the language, log in to Superset, and reset the password.
Step 5: Obtain Data from MySQL Databases for Analysis	To use Superset to obtain data from MySQL databases for analysis, you need to connect to a database, add datasets, and create charts.

Step 1: Purchase a FlexusL Instance

1. Log in to the FlexusL [console](#) and click **Buy FlexusL**.
2. Specify required parameters for the FlexusL instance.



Parameter	Example	Description
Region	CN-Hong Kong	For low network latency and quick resource access, select the region nearest to your target users. After a FlexusL instance is created, the region cannot be changed. Exercise caution when selecting a region.
Application Image	Superset	Select the Superset application image.
Instance Specifications	2 vCPUs 8 GiB memory	Select instance specifications as needed.
Instance Name	Superset-Example	Customize an instance name that is easy to identify, for example, Superset-Example.
(Optional) Associated Services	<ul style="list-style-type: none"> Data disk: 10 GiB Host security Cloud backup vault: 170 GiB 	You can bundle any of EVS, HSS (basic edition), and CBR to your FlexusL instances as needed and set specifications as needed.

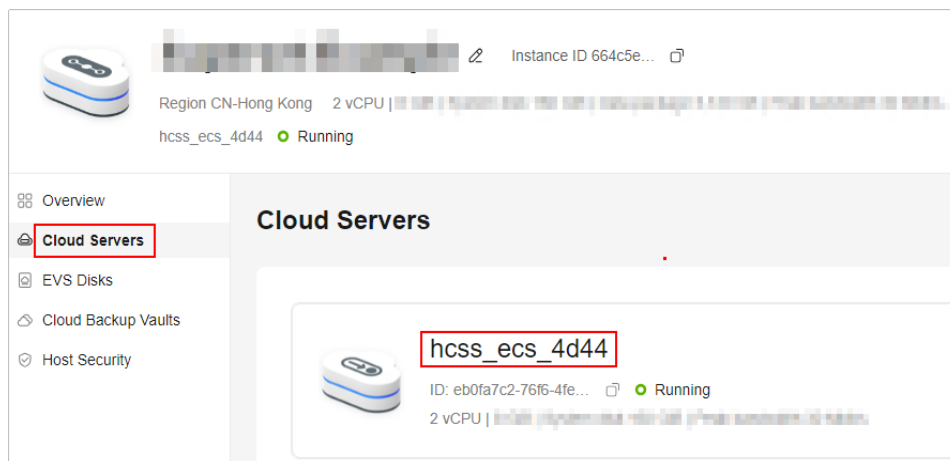
Parameter	Example	Description
Required Duration	1 month	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. For more information about auto-renewal rules, see Auto-Renewal Rules .
Quantity	1	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now** and complete the payment as prompted.
4. Go back to the FlexusL console and view the purchased FlexusL instance.

Step 2: Configure Security Groups

Add inbound security group rules to ensure that the application preinstalled in the image can be accessed.

1. Log in to the FlexusL [console](#) and click a resource card to go to the instance details page.
2. In the navigation pane on the left, choose **Cloud Servers**. Locate the server and click its name.



3. On the **Security Groups** tab, click **Add Rule**. In the displayed dialog box, add rules displayed in the following figure and click **OK**.

The following figure only displays common rules. You can add more rules as needed.

Table 4-9 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of application images
1	Allow	IPv4	TCP: 3306	0.0.0.0/0	Allows access to MySQL databases.
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M page.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

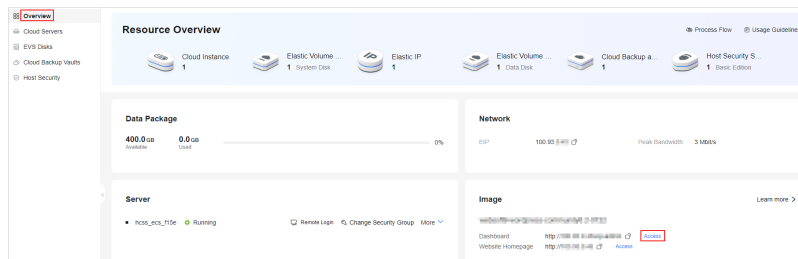
Step 3: Reset a Password

A FlexusL instance does not have an initial password. After creating a FlexusL instance, set a password for the FlexusL instance. The password of the FlexusL instance is also used for [logging in to the O&M page of the application](#).

1. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard and check whether the application has been up and running. If yes, go to the next step.

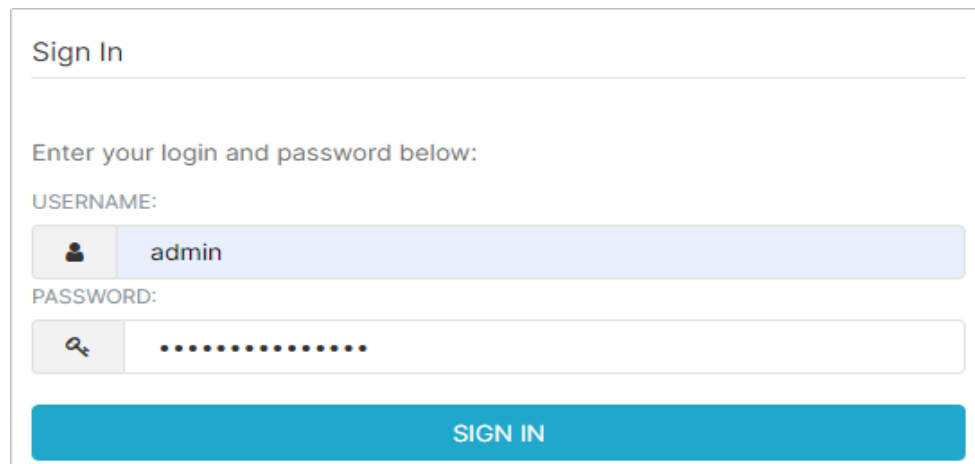
NOTICE

Wait for several minutes until the image with the pre-installed application is up and running. Then, you can perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the initial password may become invalid and you cannot log in to the application dashboard.

Figure 4-18 Entry to the application dashboard

After the application is started, the initialization wizard page of the dashboard is displayed, as shown in [Figure 4-19](#).

Figure 4-19 Initialization wizard page of the Superset dashboard



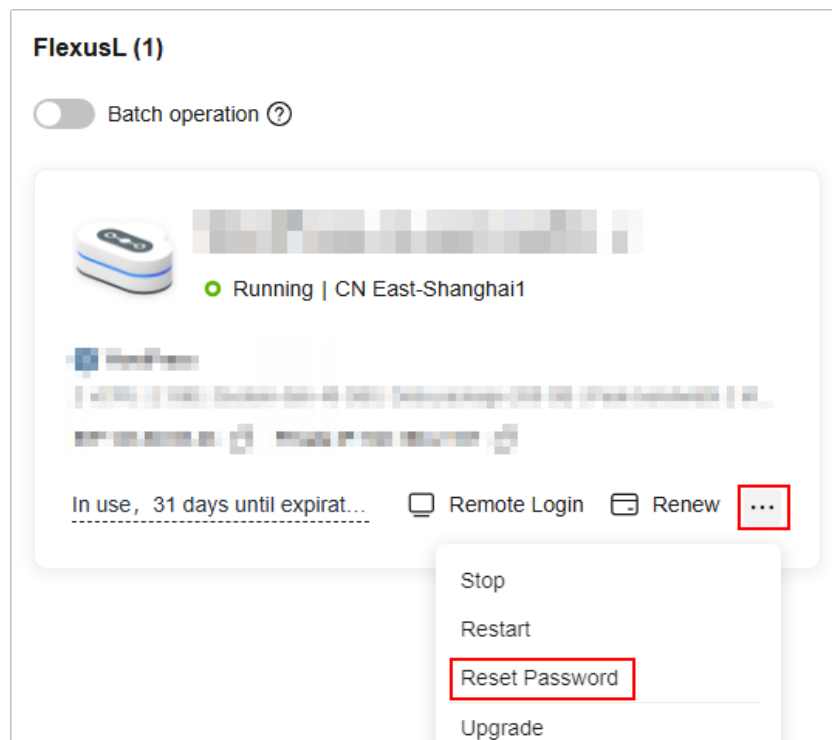
NOTE

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
 - The dashboard is being started. Try again later.
2. Locate the resource card and choose **...** > **Reset Password** to reset the password.

For details, see [Resetting the Password for a FlexusL Instance](#).

Figure 4-20 Resetting a password



NOTE

The password for logging in to the FlexusL instance is also the password for logging in to the O&M page of the application.

Step 4: Initialize Superset

Application images use code-based Ubuntu. They provide graphical user interfaces to make your operations easier. You need to initialize the application dashboard upon the first login. Then you can directly log in to the dashboard from the FlexusL console afterwards.

1. In the address bar of a local browser, enter **http://<Server-EIP>:9000** to log in to the application O&M page.

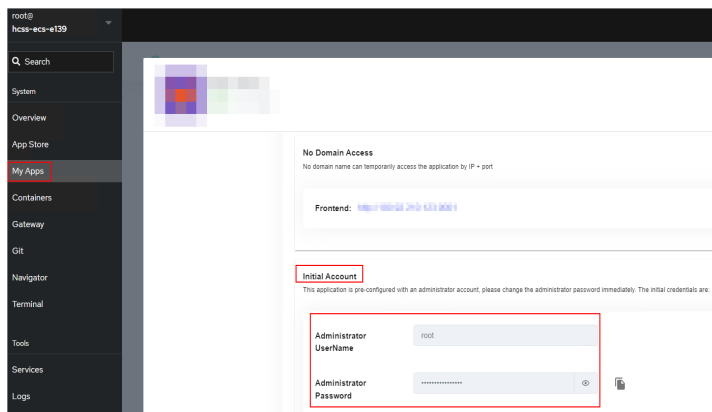
The initial username and password for logging in to the application dashboard are stored on the O&M page of the application. You need to log in to the O&M page first to obtain the username and password. The username for logging in to the O&M page is **root**, and the login password is the password reset in 2.

NOTE

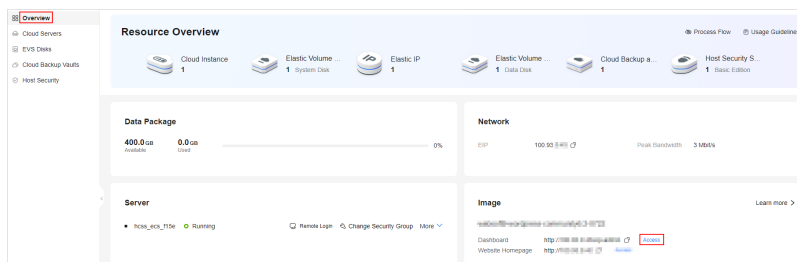
For details about the FlexusL instances, O&M page, and dashboard, see [What Is the Relationship Among FlexusL Instances, the Dashboard, and the O&M Page?](#)

2. On the **My Apps** page, click the application icon, choose **Access**, and click **Initial Account** to view the username and password for logging in to the application management page.

The initial password is a randomly generated strong password. After the application is initialized, change the password on the dashboard for easy management. If the password is changed, the initial password will be invalid. Remember the new password.



3. In the **Image** area on the **Overview** page of the FlexusL console, click **Access** to go to the application dashboard.

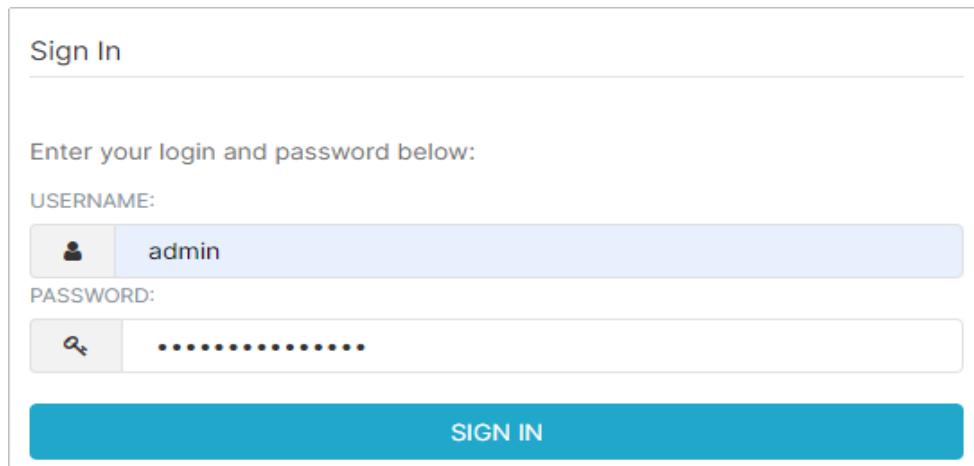


 **NOTE**

If the dashboard is not properly displayed, check the following causes:

- The port for accessing the dashboard is not allowed. Check whether the port is allowed based on [Step 2: Configure Security Groups](#).
 - The dashboard is being started. Try again later.
4. Enter the username and password obtained in 2 to access the dashboard. You can set the language on the login page or on the management page.

Figure 4-21 Initialization wizard page of the Superset dashboard



Sign In

Enter your login and password below:

USERNAME:

PASSWORD:

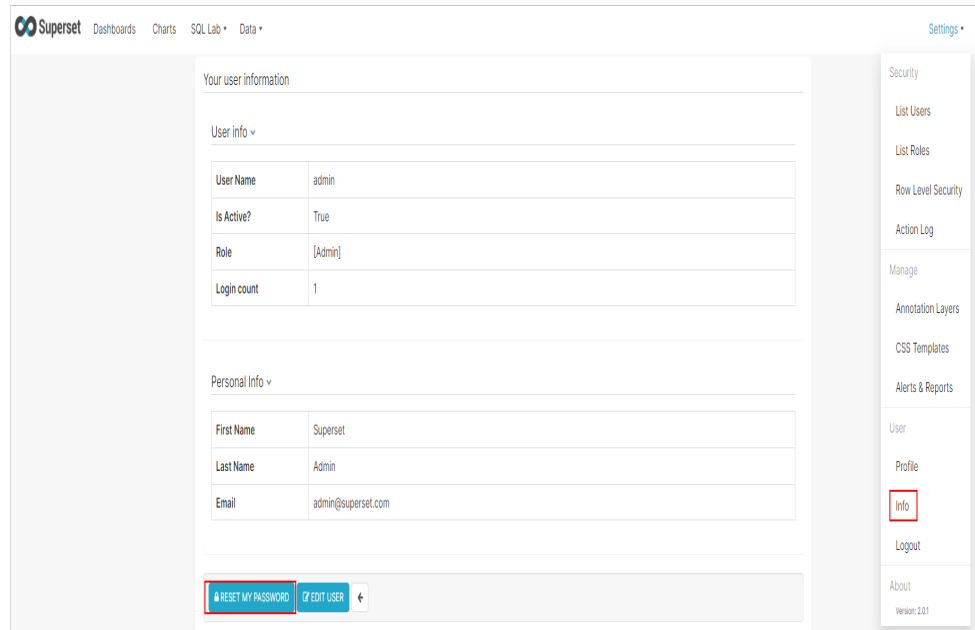
SIGN IN

 **NOTE**

If a message is displayed indicating that the username or password you entered is invalid when you attempt to log in to the application dashboard, refer to [Why Can't I Access the Dashboard of the Application Pre-installed in the Application Image After Entering the Initial Username and Password?](#)

5. In the upper right corner of the page, choose **Settings > User > Info** and click **RESET MY PASSWORD**.

Preset passwords are usually difficult to remember, so you are advised to set a password that is easy to remember, and please keep it safe.



After the Superset application is initialized, you can deploy your applications on the dashboard.

Step 5: Obtain Data from MySQL Databases for Analysis

This section describes some basic operations of Superset. For more information, see [Superset Documentation](#).

Step 1: Connect to Database

You can only analyze data after connecting to a database first.

1. On the management page, choose **Data > Databases** and click **+DATABASE**.
2. Select the database to be connected, for example, the MySQL database.
3. Enter the information about the database to be connected.

Connect a database [X]

STEP 2 OF 3

Enter the required MySQL credentials

Need help? [Learn more about connecting to MySQL.](#)

HOST * ⓘ PORT *

DATABASE NAME *

Copy the name of the database you are trying to connect to.

USERNAME *

PASSWORD ⓘ

DISPLAY NAME *

Pick a nickname for this database to display as in Superset.

ADDITIONAL PARAMETERS

Add additional custom parameters

SSL ⓘ

Table 4-10 Parameter descriptions

Parameter	Description
HOST/PORT	Specifies the public IP address and port number of the database. The default MySQL port number is 3306.
DATABASE NAME	Specifies the name of the database to be connected.
USERNAME/PASSWORD	Specifies the username and password of the database.
DISPLAY NAME	Specifies the name displayed on Superset after the database is connected.

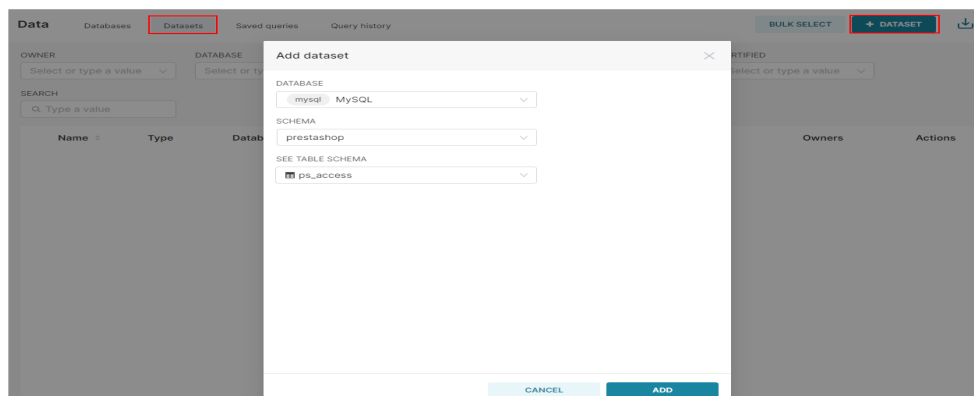
4. Click **CONNECT**.
5. Click **FINISH** and you can view the connected database in the list.

Database	Backend	AQE	DML	CSV upload	Expose in SQL Lab	Created by	Last modified
MySQL	mysql	x	x	x	✓	Superset Admin	now
examples	postgresql	x	x	x	✓		a day ago

Step 2: Add Datasets

Now that you have configured a data source, you need to register tables (called **Datasets** in Superset) for subsequent chart creation.

1. Choose **Data > Datasets** and click **+DATASET**.

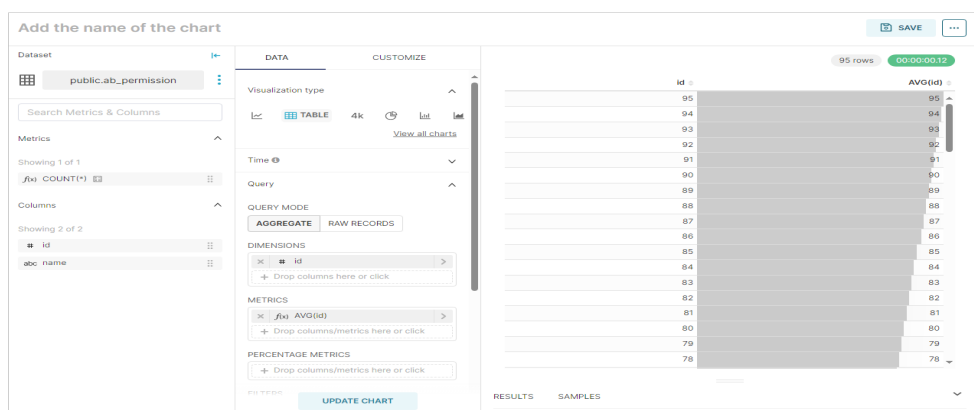


2. Click **ADD**, and you can view your dataset in the list of datasets.

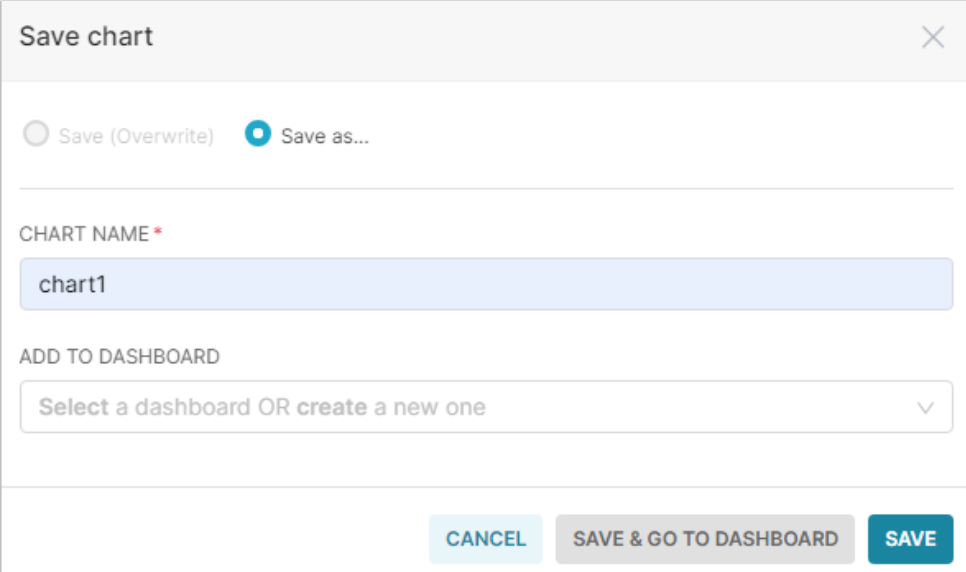
Step 3: Create Charts

Superset is a powerful visualization builder that allows you to create charts and dashboards. This section is for demonstration only. You can create exquisite charts and dashboards by referring to the [official guide](#).

1. Click the database name to visualize the chart.



2. Click **SAVE** to add the chart to the dashboard.



The image shows a 'Save chart' dialog box with a close button (X) in the top right corner. It contains two radio buttons: 'Save (Overwrite)' which is unselected, and 'Save as...' which is selected. Below this is a text input field labeled 'CHART NAME *' containing the text 'chart1'. Underneath is a dropdown menu labeled 'ADD TO DASHBOARD' with the text 'Select a dashboard OR create a new one' and a downward arrow. At the bottom, there are three buttons: 'CANCEL' (light blue), 'SAVE & GO TO DASHBOARD' (grey), and 'SAVE' (dark blue).

3. Click **SAVE & GO TO DASHBOARD**. The visualized chart is displayed on the dashboard.

5 Server Migration

5.1 Using Images to Migrate FlexusL Instances to ECSs

Scenarios

A FlexusL instance is a lightweight application server. It is friendly to beginners in cloud computing. However, the instance specifications and functions are limited. If a FlexusL instance does not meet your service requirements, you can change the FlexusL instance to an ECS to obtain more specifications and functions. This practice uses IMS to create an image from a FlexusL instance and then uses the image to quickly create an ECS with the same configurations as the FlexusL instance. In this way, your application is migrated from the FlexusL instance to the ECS.

The following describes how to migrate a FlexusL instance with Nginx deployed to an ECS using an image.

Resource Planning and Costs

This practice uses the following resource planning as an example. You can adjust it as required.

Resource	Configuration	Description	Cost
Source FlexusL instance	Region: CN North-Beijing4	Resources will be migrated from the source FlexusL instance.	Billing is not involved for existing resources.

Resource	Configuration	Description	Cost
Image	Image name: flexusl-image	If the FlexusL instance contains only a system disk, create a system disk image. If the FlexusL instance also contains a data disk, create a full-server image.	If the FlexusL instance is not associated with a backup vault, a small amount of pay-per-use expenditures are involved during the creation of the full-server image.
ECS	<ul style="list-style-type: none">Region: CN North-Beijing4ECS name: ecs-flexusl	The ECS is created using the image.	For details about the expenditures required for purchasing an ECS, see Price Calculator .

Constraints

- The image of the FlexusL instance uses the x86 architecture, so the FlexusL instance can be migrated only to an x86 ECS.
- When migrating the FlexusL instance to an ECS, ensure that the memory of the ECS is greater than or equal to the memory or memory usage of the FlexusL instance. Otherwise, the ECS may be unavailable due to insufficient memory.

Process

Procedure	Description
Step 1: Create a FlexusL Instance Full-Server Image	Create an image from the FlexusL instance and use the image to quickly provision ECSs with the same configurations.
Step 2: Create an ECS Using an Image	Use the image to create an ECS with the same configurations and verify services.
Step 3: Release Related Resources	Release the source FlexusL instance and the resources generated during the migration.

Step 1: Create a FlexusL Instance Full-Server Image

- On the [IMS console](#), click **Create Image**.
- Configure image parameters.

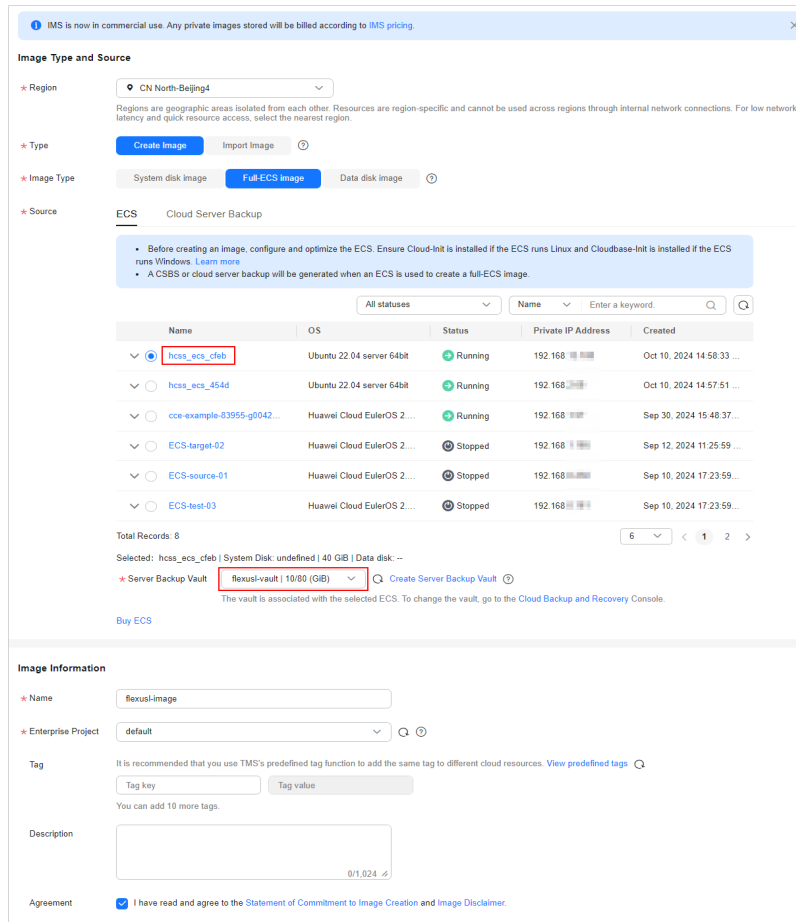


Table 5-1 Image parameters

Parameter	Example Value	Description
Image Type and Source		
Region	CN North-Beijing4	Select the region where the source FlexusL instance is located.
Type	Create Image	When creating an image for a server on Huawei Cloud, select Create Image .
Image Type	Full-ECS image	<ul style="list-style-type: none"> If your FlexusL instance only contains a system disk, select System disk image. System disk images can be created more quickly, and you do not need to pay for server backup vaults. If your FlexusL instance contains both a system disk and a data disk, create a full-server image.

Parameter	Example Value	Description
Source	On the Servers tab: <ul style="list-style-type: none"> Cloud server: hcss_ecs_454d Server backup vault: flexusl-vault 	Click the Cloud Server tab and perform the following operations: <ul style="list-style-type: none"> Select the cloud server name of the FlexusL instance where an image is to be created. Server backup vault: Click the drop-down list to select an available vault. If no vault is available, click Create Server Backup Vault to create a vault. For details about the parameters, see Table 5-2. After purchasing a vault, click the refresh button on the right of the selection box and select the vault. <p>NOTE If you create a system disk image, Server Backup Vault is unavailable.</p>
Image Information		
Name	flexusl-image	Customize an image name that is easy to be identified.
Enterprise Project	default	default

Table 5-2 Server backup vault parameters

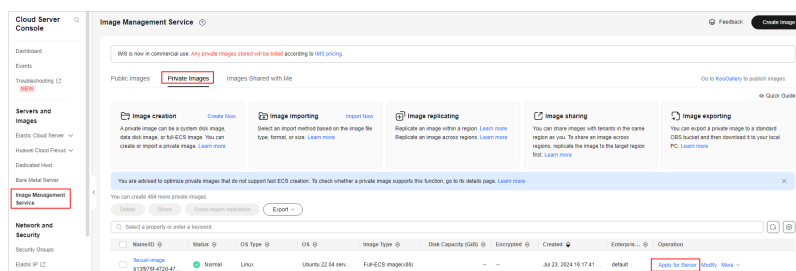
Parameter	Example Value	Description
Billing Mode	Pay-per-use	Select a cloud server backup billing mode.
Region	CN North-Beijing4	The region is fixed.
Protection Type	Retain the default setting Backup	Backup vaults store the backup data of protected resources.
Application-Consistent Backup	Retain the default setting to disable this option.	Set this parameter based on the site requirements. It is not enabled by default.

Parameter	Example Value	Description
Backup Data Redundancy	Retain the default value Single-AZ.	Select a value based on site requirements. The single-AZ backup is used as an example.
Resources to Backup	<ul style="list-style-type: none"> Configure hcss_ecs_454d 	Associate the cloud server of the FlexusL instance to be backed up with the vault.
Backup Capacity	80 GiB	Set this parameter based on site requirements. The vault capacity must be greater than the capacity of the FlexusL instance to be backed up, or the backup may fail.
Backup Policy	Skip	Set this parameter based on the site requirements. It is not configured in this example
Enterprise Project	default	default
Vault Name	flexusl-vault	In Advanced Settings , you only need to customize the vault name.

3. Click **Next** and create an image as prompted.

Step 2: Create an ECS Using an Image

1. On the **IMS console**, select the created private image **flexusl-image** and click **Apply for Server** in the **Operation** column.



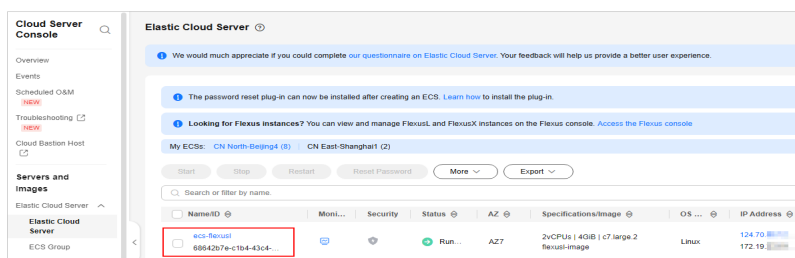
2. On the page for purchasing an ECS, select the ECS specifications and parameters as required, and click **Submit**.

For an ECS requested from IMS, retain the default region settings and fixed image settings. For details about other parameters, see **Purchasing a Custom ECS**.

NOTE

- Images are regional resources. ECSs can only be created from the images that are in the same region as them. If you want to create ECSs using the image in other regions, replicate the image to other regions before creating ECSs by referring to [Replicating Images Across Regions](#).
- The image of the FlexusL instance uses the x86 architecture, so the FlexusL instance can be migrated only to an x86 ECS.
- When migrating the FlexusL instance to an ECS, ensure that the memory of the ECS is greater than or equal to the memory or memory usage of the FlexusL instance. Otherwise, the ECS may be unavailable due to insufficient memory.

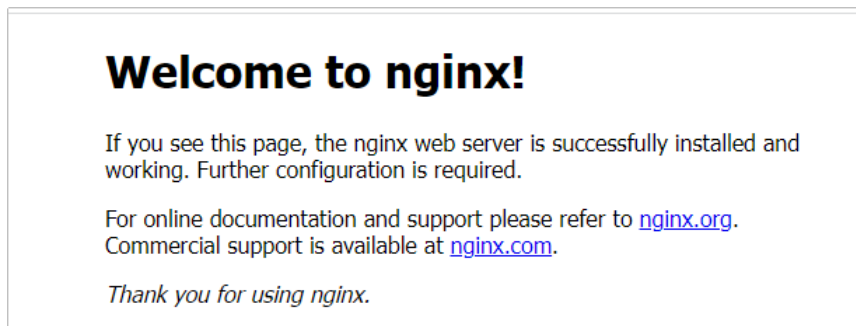
3. Click **Back to ECS List**. The created ECS is displayed in the ECS list.



4. After the migration, check whether services are normal.

Copy the EIP of the migrated server and use a browser to access the Nginx service. If the Nginx service can be accessed, the migration is successful.

The Nginx server is manually deployed in the source FlexusL instance. This section uses the Nginx server as an example to describe how to verify services after the migration is complete. Perform the verification based on the actual services of your FlexusL instance.

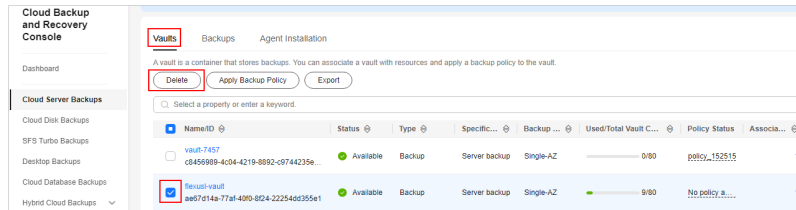
**Step 3: Release Related Resources**

- Unsubscribe from the source FlexusL instance. For details, see [Unsubscribing from FlexusL Instances](#).
- Delete a cloud backup vault.

On the CBR console, locate the **created server backup vault** and click **Delete**.

NOTE

If you have created a system disk image, skip this step because this resource is not involved during server migration.



5.2 Using SMS to Migrate Servers to FlexusL Instances

Application Scenario

This section describes how to use Server Migration Service (SMS) to migrate other cloud servers to Huawei Cloud FlexusL instances in the same region or across regions.

Precautions

- Once the migration starts, do not perform operations on the FlexusL instances, including but not limited to stopping the instances, changing the OS, or reinstalling the OS. Otherwise, the migration will be interrupted or fail.
- If you want to migrate incremental data after the full migration is complete, do not reinstall or change the OS for the FlexusL instances, or the migration will fail.

Constraints

- Only x86 servers can be migrated to FlexusL instances.
- SMS migrates entire servers. It cannot only migrate system or data disks of servers.
- Only servers with one data disk can be migrated. The paired FlexusL instances must have system and data disks at least as large as the source servers.

For more information, see [SMS Precautions](#) and [SMS Constraints](#).

Resource Planning and Costs

Resource	Data Planning	Description	Cost
Source server	Server name: source-server OS: CentOS 7.9	The source server can be in Huawei Cloud, another cloud platform, or an on-premises environment.	If the source server has no EIP bound, you need to configure one for the source server. You need to pay for the EIP.

Resource	Data Planning	Description	Cost
Target server	Server name: destination_server OS: Huawei Cloud EulerOS 2.0	The target server is a Huawei FlexusL instance.	You need to pay for the FlexusL instance.
SMS	-	SMS is available for free.	You need to pay for the pay-per-use migration resources (including EVS disks, EVS snapshots, and traffic) used during the migration. For details, see SMS Billing .

Process

Procedure	Description
Making Preparations	Prepare accounts, obtain required permissions, and prepare source and target servers.
Step 1 Installing and Starting the Agent on the Source Server	Install and start the Agent on the source server. To start the Agent, you must enter the AK/SK pair of the Huawei Cloud account the FlexusL instance belongs to. After the Agent is started, it reports information about the source server to SMS.
Step 2: Configuring the Target Server on the SMS Console	Configure the target server which will receive data migrated from the source server.
Step 3: Starting the Migration	Start the migration to replicate all data from the source server to the target server. The replication speed depends on the outbound bandwidth of the source server or the inbound bandwidth of the target server, whichever is smaller.
Step 4: Viewing the Migration Result	Check whether the source server is successfully migrated, and install the one-click password reset plug-ins and the HSS Agent on the target server.
Step 5: Creating a Private Image and Changing the OS of the FlexusL instance	Create a private image for the FlexusL instance and use the image to change the OS for the instance. In this way, the OS name of the FlexusL instance can be displayed in the instance card, and reinstalling the OS for the FlexusL instance will not roll back its OS to that before the migration.

Making Preparations

Prepare accounts, obtain required permissions, and prepare source and target servers.

1. [Register a HUAWEI ID and enable Huawei Cloud services.](#)

 **NOTE**

[Real-name authentication](#) is required for migration to regions within the Chinese mainland.

2. Obtain required permissions for your HUAWEI ID.

If you use an HUAWEI ID for migration, you have the required permissions by default. If you use an IAM user for migration, you need to obtain the required permissions. For more information, see [Creating a User Group and Assigning Permissions](#).

3. Obtain an AK/SK pair for your target account.

The AK/SK pair will be used for authentication during the migration. To learn how to obtain an AK/SK pair, see [How Do I Obtain an AK/SK Pair for an Account?](#)

 **CAUTION**

SMS does not support AK/SK-based authentication for federated users (virtual users).

-
4. Note the username and password for logging in to the source server.

If your source server is not in Huawei Cloud, note the username and password of the source server. The username and password are required when you install the one-click password reset plug-ins on the target server after the migration is complete. If you forget the username and password, the plug-ins installation process will be complex.

5. Confirm that the source server OS is supported by SMS.

- See [Supported Windows OSs](#) or [Supported Linux OSs](#).
- A target server must run the same type of OS as the source server.

6. Ensure that the following network requirements are met:

- a. The source server can connect to the Huawei Cloud API Gateway over TCP port 443. For more information, see [Connecting Source Servers to Huawei Cloud API Gateway](#).

 **NOTE**

It is recommended that all outbound ports on the source server be opened.

- b. The source server can connect to the target server. For more information, see [Connecting Source Servers to Target Servers](#).

In this practice, EIP is used for connection. You need to purchase and configure EIPs for both the source and target servers. A FlexusL instance has an EIP bound by default.

- c. The following ports are enabled in the security group of the target server to allow traffic to these ports:
- Windows: TCP ports 8899, 8900, and 22
 - Linux: TCP port 22 for file-level migration, and ports 8900 and 22 for block-level migration

For details about how to control traffic into and out of a security group, see [Adding a Security Group Rule](#).

CAUTION

- For security purposes, you are advised to only allow traffic from the source servers over these ports.
- The firewall of the target server must allow traffic to these ports.

-
7. Ensure that the following source server requirements are met:

Available Space

- Windows: at least 320 MB of available space on a partition not smaller than 600 MB, and at least 40 MB of available space on a partition smaller than 600 MB
- Linux: at least 200 MB of available space on the root partition

Source Environment

- The system time of the source server must be consistent with the local standard time to avoid Agent registration failures.
- If the source server runs Linux, **rsync** must be installed on it. You can run the **rsync -v** command to check whether **rsync** is installed.

If it is not, install it by running the following command:

- CentOS: **yum -y install rsync**
- Ubuntu: **apt-get -y install rsync**
- Debian: **apt-get -y install rsync**
- SUSE: **zypper install rsync**
- Other distributions: Refer to the official website documentation.

 **NOTE**

rsync comes preinstalled on most distributions by default.

Step 1 Installing and Starting the Agent on the Source Server

- If the source server runs a Linux OS, see [Installing the Agent on Linux](#).
- If the source server runs a Windows OS, see [Installing the Agent on Windows](#).

FAQ

1. If an error message indicating that rsync is not installed is displayed when you install Agent on the Linux source server, install rsync based on [Installing Rsync](#) and then reinstall the Agent.

```
[root@ecs-migrate-to-hecs SMS-Agent]# ./startup.sh
Start the migration pre-check. Please waiting...                               ko
[ 1165.691808] device-mapper: uevent: version 1.0.3
[ 1165.692860] device-mapper: ioctl: 4.37.1-ioctl (2018-04-03) initialised: dm-devel@redhat.com
[ 1166.034082] SGI XFS with ACLs, security attributes, no debug enabled
[ 1166.059118] xor: automatically using best checksumming function:
[ 1166.069340]   avx      : 25480.000 MB/sec
[ 1166.092340] raid6: sse2x1   gen() 10550 MB/s
[ 1166.109342] raid6: sse2x2   gen() 15179 MB/s
SMS-Age126340ntraid6: sse2x4   gen() 19589 MB/s
SMS-Age143340ntraid6: avx2x1   gen() 21898 MB/s
SMS-Age160330ntraid6: avx2x2   gen() 30839 MB/s
SMS-Age177330ntraid6: avx2x4   gen() 34250 MB/s
SMS-Age194a30ntraid6: cavx512x1 gen() 28093 MB/s;x86_64/iocapture.ko
SMS-Age211a39nt/ioblocavx512x26.32-7133218x86_64/
SMS-Age228a30nt/ioblocavx512x46.32-7140242x86_64/iocapture.ko
SMS-Age228780nt/ioblocusing algorithm avx512x4 gen() (40242 MB/s)
SMS-Age229355nt/x86/ using avx512x2 recovery algorithm
SMS-Age273780ntBtrfs loaded, crc32c=crc32c-intel
SMS-Age282437ntfuse init (API version 7.23)
checking migration risks ...

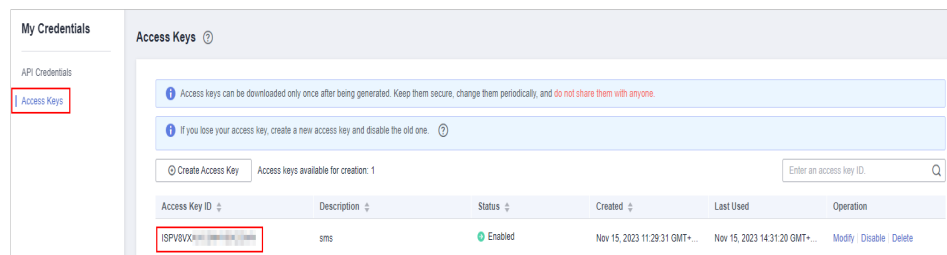
Pre-migration failed. The following problems are found:
LinuxCheckBeforeStartup:
Error!!! SMS.6517: rsync not installed on the source server.
```

2. If the following error message is displayed, check whether the access key is correctly entered or deleted.

Figure 5-1 Error message

```
After the SMS-Agent is started, the SMS-Agent performs a migration check, collects the system configuration, hardware, disk, and IP address information of the source server, and reports the collected information to SMS. All information collected is used for data migration only and will not be used for other purposes. You can delete a migration task on the SMS console at any time. The system automatically deletes all the preceding information. Do you agree? (y/n)y
Please input AK(Access Key ID) of Public Cloud:QJ0F8UG6FUYSP4GWL1HL
Please input SK(Secret Access Key) of Public Cloud:*****
sms.cn-north-4.mhuaweicloud.com
Do you want to use the sms_domain you entered last time? Please enter Y/y or N/n: n
Please input sms_domain of Public Cloud: sms-*****.com
agent is starting, this may take a few minutes...
Failed to obtain the JSON configuration file, incorrect SMS domain name. Ensure that the system time is consistent with the standard time and the AK and SK are correct. Please check the entered voucher or network Failed to start sms agent!root@ecs-migrate-to-hecs SMS-Agent]#
```

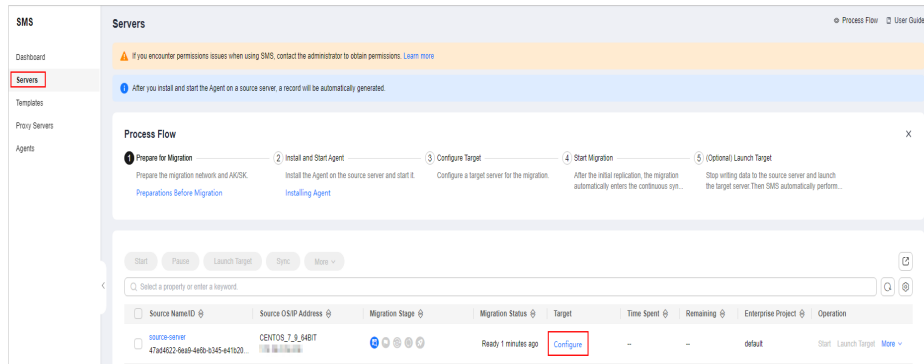
Figure 5-2 Access key



Step 2: Configuring the Target Server on the SMS Console

1. Log in to the [SMS console](#) using the Huawei Cloud account that owns the FlexusL instance and choose **Servers** on the left.
2. On the **Servers** page, locate the source server to be migrated and click **Configure**.

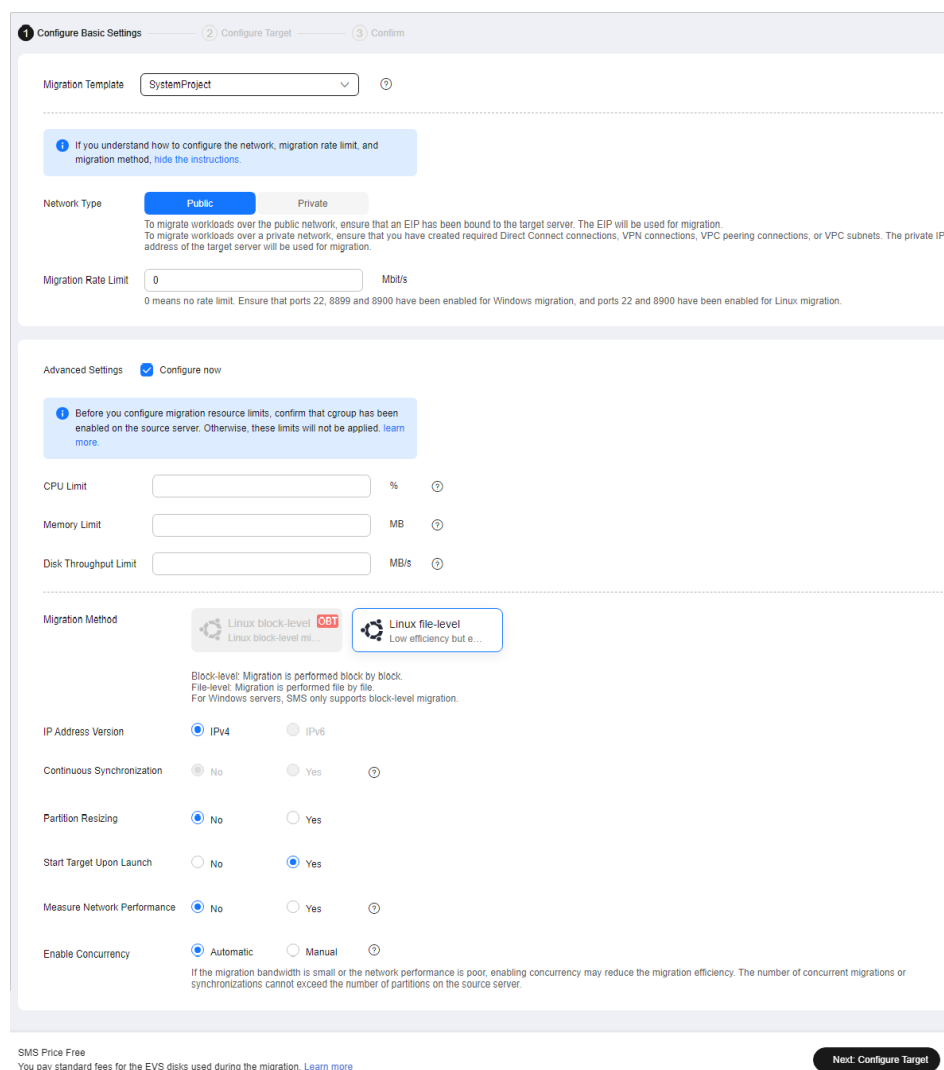
After step 1 is complete, you can see the source server record on the **Servers** page of the SMS console.



3. Configure the basic settings.

Retain the default settings on this page.

For details about the parameters, see [Configuring the Target Server](#).



4. Configure the target server and click **Next: Confirm** in the lower right corner.

- **Region:** Select the region where the purchased FlexusL instance is located.
- **Server:** Select **Use existing** and choose the purchased FlexusL instance.

- Only servers with one data disk can be migrated. The paired FlexusL instances must have system and data disks at least as large as the source servers.
- The target server must run the same type of OS as the source server.
- The security group of the target server must be correctly configured. It must be configured to allow access on TCP ports 8899, 8900, and 22 for a Windows migration, or on port 22 for a Linux migration.

Configure Basic Settings — 2 Configure Target — 3 Confirm

Region: CN South-Guangzhou

Project: cn-north-4-(default)

Server: Use existing (selected) | Create new

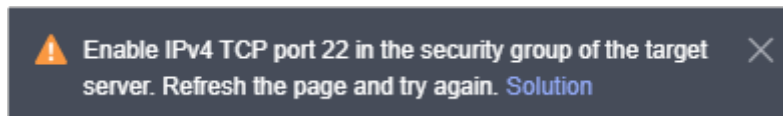
1. If you select Create new, a pay-per-use ECS will be created by default. You can change its billing mode to yearly/monthly after the migration is complete.
2. If you switch services over to a cloned target server, the target server will use the same login credentials as the source server.
To ensure that the target can start properly after migration, the target server will be formatted during migration, and such information as the registry and network configuration will be modified. Advised to back up data before migration.

Name: For a global search, enter a name. | For a search on the current page, enter a keyword.

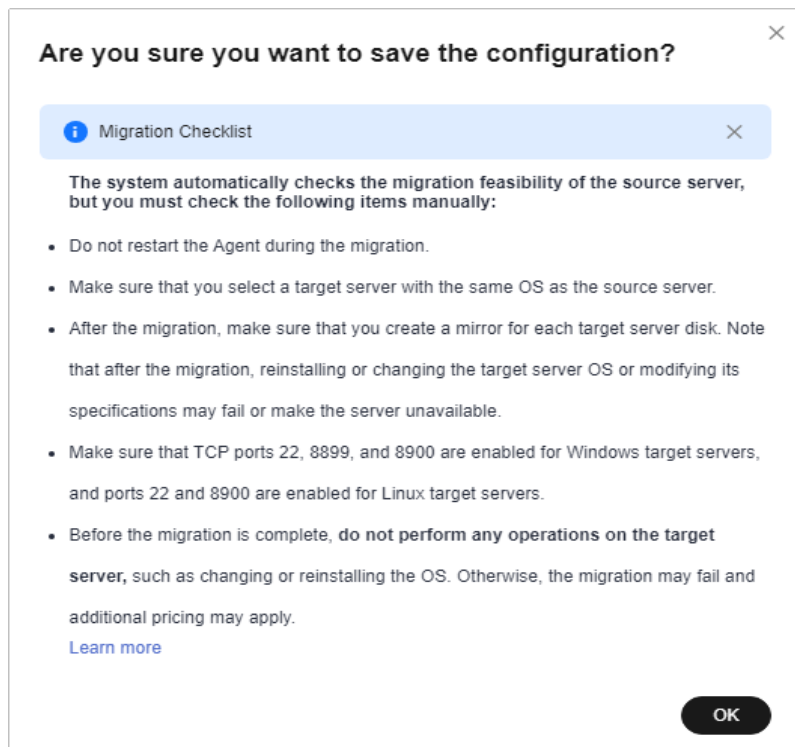
Source: source-server | Recommended Target: OS: CENTOS_7_9_64BIT | System Disk: 40 GIB | Create Now

Name	OS	Disk	Private IP Address	EIP
hcss_ecs_23eb	Huawei Cloud EulerOS 2.0 64bit	System Disk: 40 GIB		

If the following information is displayed when you perform this step, allow traffic over the prompted port, refresh the page, and repeat this step.



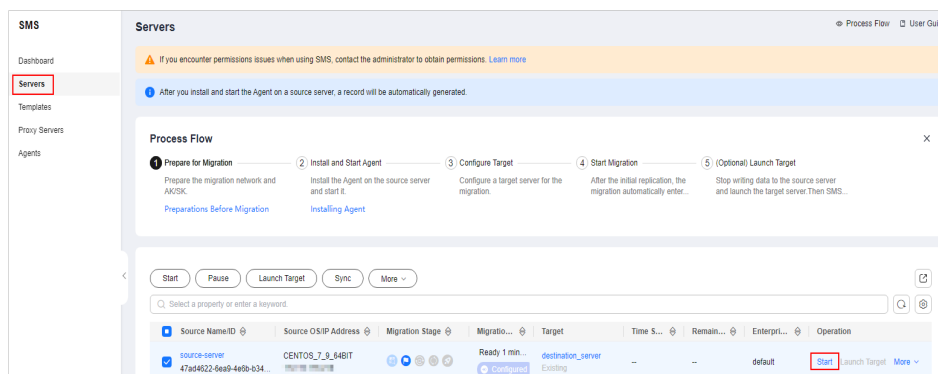
5. On the **Confirm** page, confirm the information and click **Save** or **Save and Start**.
 - If you select **Save**, read the migration checklist carefully and click **OK**. Then **start the migration**.
 - If you select **Save and Start**, read the migration checklist carefully and click **OK**. The migration starts automatically. **View the migration status and details**.



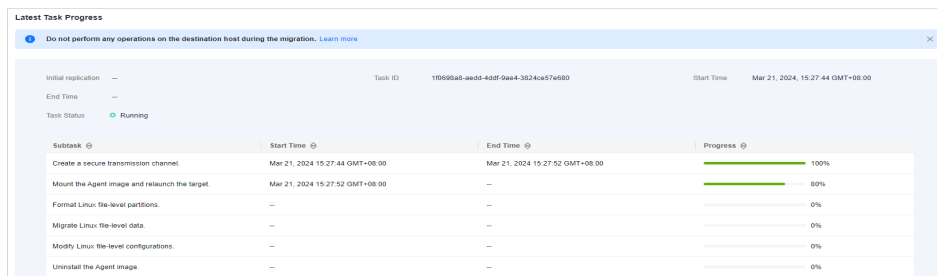
Step 3: Starting the Migration

1. Log in to the [SMS console](#) using the Huawei Cloud account that owns the FlexusL instance and choose **Servers** on the left.
2. On the **Servers** page, locate the source server to be migrated and click **Start** in the **Operation** column.

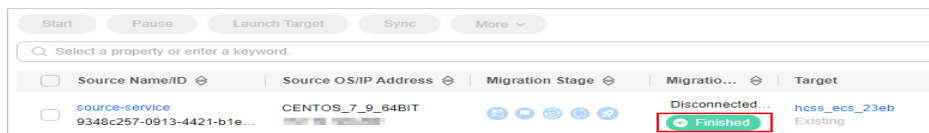
Alternatively, select the server to be migrated and click **Start** above the server list.



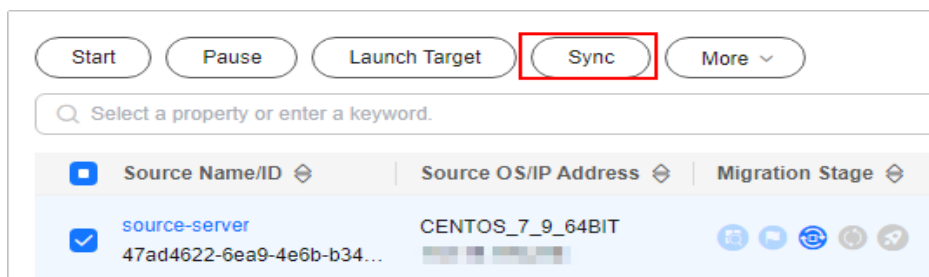
3. After the migration starts, click the name of the source server to view the migration status and details.



4. Check whether the **Status** changes to **Finished**. If it changes, the target server has been launched, and the migration is complete.



5. (Optional) If incremental data is generated on the source server after the full migration is complete, synchronize the incremental data from the source server to the target server.

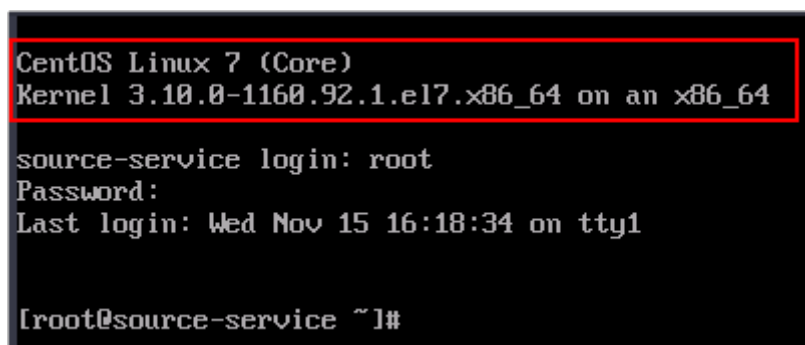


NOTE

If you want to migrate incremental data after the full migration is complete, do not reinstall or change the OS for the target server, or the migration will fail.

Step 4: Viewing the Migration Result

1. Check the OS on the FlexusL instance.
Click **Remote Login** in the FlexusL instance card. If the OS and kernel information of the source server is displayed, the migration is successful.
Enter the username and password of the source server to log in to the FlexusL instance.

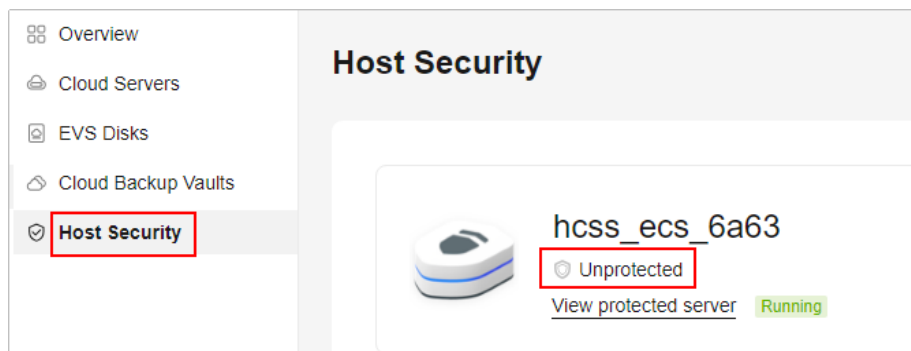


2. (Optional) Install the one-click password reset plug-in on the FlexusL instance.

If your source server was not created from a Huawei Cloud image, install the one-click password reset plug-in on the FlexusL instance. With the plug-in, you can reset your instance password. To install the plug-in, refer to the following:

- [What Should I Do If the Password Cannot Be Reset After I Use a Private Linux Image to Create a FlexusL Instance or Change the OS of an Existing Instance and I Forgot the Initial Password of the Private Image?](#)
 - [What Should I Do If the Password Cannot Be Reset After I Use a Private Linux Image to Create a FlexusL Instance or Change the OS of an Existing Instance and I Know the Initial Password of the Private Image?](#)
3. (Optional) Check the HSS service status.
- If your FlexusL instance does not contain the HSS service, skip this step.
 - If your FlexusL instance contains the HSS service, but the service is not enabled, enable HSS by referring to [What Do I Do If HSS Is Not Started After I Use a Private Image to Create a FlexusL Instance or Change the OS of an Instance?](#)

Figure 5-3 HSS Unprotected status



Step 5: Creating a Private Image and Changing the OS of the FlexusL instance

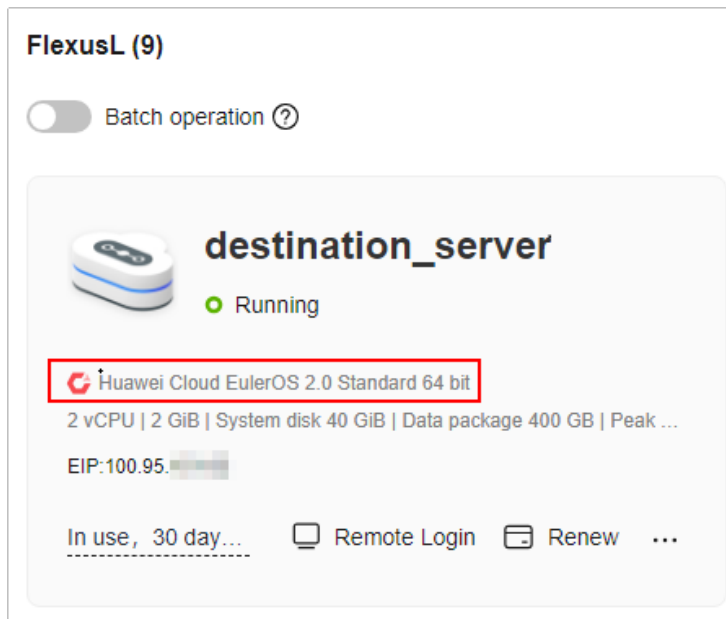
After the migration is complete, the original OS name (Huawei Cloud EulerOS 2.0) is still displayed in the FlexusL instance card, as shown in figure [Figure 5-4](#). If you choose to reinstall the OS for the FlexusL instance after the migration is complete, the OS will actually be rolled back to the original OS Huawei Cloud EulerOS 2.0 rather than CentOS 7.9, and the OS data migrated from the source server will be lost.

Create a private image for the FlexusL instance. Then use the image to change the OS for the instance. After the OS is changed, the above two problems can be solved.

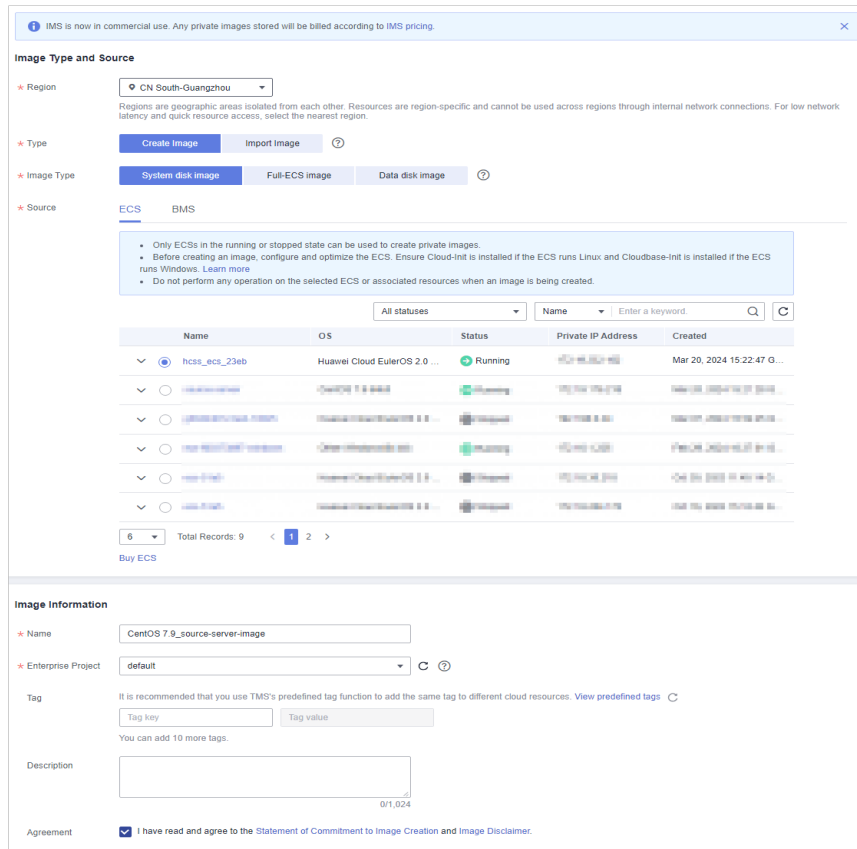
NOTICE

If the OS is changed, incremental data on the source server cannot be synchronized. Ensure that no incremental data needs to be synchronized before changing the OS.

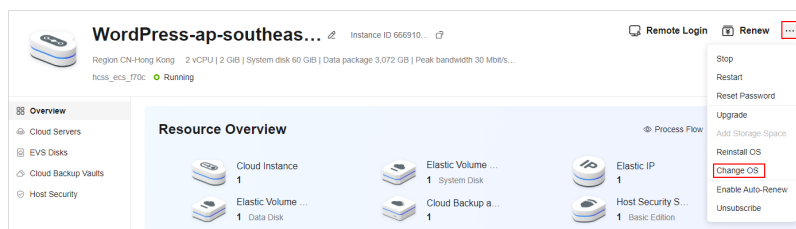
Figure 5-4 Image name of the FlexusL instance



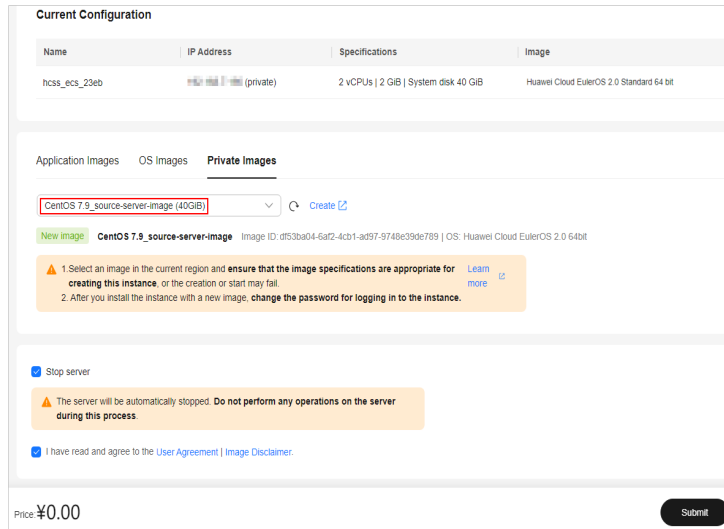
1. Log in to [IMS console](#), choose **Create Image**, and configure the following parameters:
 - **Region:** Retain the default value.
 - **Type:** Retain the default value.
 - **Image Type:** Retain the default value.
 - **Source:** Select the FlexusL instance.
 - **Name:** Enter an image name that is easy to identify, for example, **CentOS 7.9_source-server-image**.
 - **Agreement:** Read the agreements and select the **Agreement** option.



2. Click **Next**, confirm the information, and click **Submit**.
3. Go back to the FlexusL console, click the FlexusL instance, and choose **Change OS** in the upper right corner.



4. Configure the parameters for changing the OS and click **Submit**.
 - Select the private image **CentOS 7.9_source-server-image** created in 1.
 - Stop the instance first or select **Stop server** on the **Change OS** page.
 - Read and agree to the agreements.



5. Check whether the image name on the console is changed.

