

Huawei Cloud Flexus

User Guide

Issue 04
Date 2024-05-30



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

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

Trademarks and Permissions



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

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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 FlexusL.....	1
1.1 Purchase a FlexusL Instance.....	1
1.2 Remotely Logging In to a FlexusL Instance Server.....	3
1.2.1 Overview.....	3
1.2.2 Remotely Logging In to a FlexusL Instance Server (Using VNC).....	6
1.2.3 Logging In to a FlexusL Instance Linux Server (Using CloudShell).....	7
1.3 Managing FlexusL Instances.....	11
1.3.1 Upgrading a FlexusL Instance.....	11
1.3.2 Searching for a FlexusL Instance.....	13
1.3.3 Renewing a FlexusL Instance.....	16
1.3.3.1 Overview.....	16
1.3.3.2 Manually Renewing FlexusL Instances.....	17
1.3.3.3 Auto-renewing a FlexusL Instance.....	20
1.3.4 Unsubscribing from a FlexusL Instance.....	23
1.4 Managing Cloud Servers.....	26
1.4.1 Managing an Instance Lifecycle.....	26
1.4.2 Viewing Cloud Server Details.....	28
1.4.3 Setting or Resetting a Password.....	29
1.4.4 Reinstalling an OS.....	31
1.4.5 Batch Reinstalling OSs.....	32
1.4.6 Changing an OS.....	37
1.5 Managing Security Groups.....	40
1.5.1 Changing a Security Group.....	40
1.5.2 Configuring Security Group Rules.....	41
1.5.3 Configuring Security Groups for Application Images.....	47
1.6 Managing Images.....	52
1.6.1 Managing Application Images.....	52
1.6.2 Managing Private Images.....	54
1.7 Managing Disks.....	58
1.7.1 Viewing Disk Information and Supported Operations.....	58
1.7.2 Expanding Capacity of a Data Disk.....	58
1.7.3 Adding a Data Disk.....	60
1.8 Managing Backups.....	61

1.8.1 Viewing Backup Information and Supported Operations.....	61
1.8.2 Associating a FlexusL Instance with a Server Backup Vault.....	63
1.8.3 Backing Up and Restoring a FlexusL Instance.....	63
1.8.4 Expanding the Vault Capacity.....	67
1.9 Managing Domain Names.....	68
1.9.1 Overview.....	68
1.9.2 Adding a Domain Name.....	69
1.9.3 Resolving a Domain Name.....	70
1.10 Managing Server Security.....	72
2 FlexusX.....	73
2.1 Purchasing a FlexusX Instance.....	73
2.2 Logging In to a FlexusX Instance.....	79
2.2.1 Remotely Logging In to a FlexusX Instance Using VNC.....	79
2.3 Managing FlexusX Instances.....	80
2.3.1 Viewing Details of a FlexusX Instance.....	80
2.3.2 Resetting a Password.....	80
2.3.3 Viewing Failures.....	83
2.3.4 Reinstalling an OS.....	84
2.3.5 Changing an OS.....	85
2.3.6 Modifying FlexusX Instance Specifications.....	87
2.3.7 Managing a FlexusX Instance Group.....	90
2.4 Managing Images.....	93
2.4.1 Overview.....	93
2.4.2 Creating a FlexusX Instance from a Private Image or Using a Private Image to Change the OS.....	95
2.4.3 Creating an Image from a FlexusX Instance.....	97
2.5 Managing EVS Disks.....	100
2.5.1 Overview.....	100
2.5.2 Adding an EVS Disk to a FlexusX Instance.....	101
2.5.3 Attaching EVS Disks to a FlexusX Instance.....	102
2.5.4 Detaching an EVS Disk from a FlexusX Instance.....	103
2.5.5 Expanding the Capacity of an EVS Disk.....	104
2.6 Managing Backups.....	105
2.6.1 Overview.....	105
2.6.2 Associating a FlexusX Instance with a Backup Vault.....	106
2.6.3 Backing Up a FlexusX Instance.....	108
2.7 Managing VPCs.....	109
2.7.1 What Is Virtual Private Cloud?.....	109
2.7.2 Attaching Extension Network Interfaces.....	110
2.7.3 Detaching Extended Network Interfaces.....	111
2.7.4 Changing a VPC.....	112
2.7.5 Changing a Private IP Address.....	114
2.7.6 Assigning a Virtual Private IP Address.....	115

2.8 Managing EIPs.....	116
2.8.1 Elastic IP Overview.....	116
2.8.2 Binding an EIP.....	117
2.8.3 Unbinding an EIP.....	118
2.8.4 Modifying a Bandwidth.....	118
2.9 Managing Security Groups.....	121
2.9.1 Security Group.....	122
2.9.2 Configuring Security Group Rules.....	123
2.9.3 Changing a Security Group.....	125
2.10 Managing Server Security.....	126
2.11 Managing Server Monitoring.....	128
2.11.1 Overview.....	128
2.11.2 Configuring an Alarm Rule.....	129
2.11.3 Viewing Server Monitoring Metrics.....	130
3 FlexusRDS.....	132
3.1 Buying a FlexusRDS Instance.....	132
3.2 Connecting to a FlexusRDS Instance.....	135
3.2.1 Using DAS to Connect to a FlexusRDS Instance (Recommended).....	135
3.2.2 Using CLI to Connect to a FlexusRDS Instance.....	136
3.3 Managing FlexusRDS Instances.....	139
3.3.1 Suggestions on Using FlexusRDS.....	139
3.3.1.1 Instance Usage Suggestions.....	139
3.3.1.2 Database Usage Suggestions.....	140
3.3.2 Database Migration.....	144
3.3.2.1 Migrating Data to FlexusRDS Using mysqldump.....	144
3.3.2.2 Migrating Data to FlexusRDS Using the Export and Import Functions of DAS.....	148
3.3.3 Permissions Management.....	151
3.3.3.1 Creating a User and Granting Permissions.....	151
3.3.3.2 FlexusRDS Custom Policies.....	152
3.3.4 Instance Modifications.....	153
3.3.4.1 Changing a DB Instance Name.....	153
3.3.4.2 Rebooting DB Instances.....	153
3.3.4.3 Resetting the Administrator Password.....	154
3.3.4.4 Storage Autoscaling.....	156
3.3.4.5 Binding and Unbinding an EIP.....	158
3.3.4.6 Renewing DB Instances.....	158
3.3.4.7 Unsubscribing a Yearly/Monthly DB Instance.....	159
3.3.5 Backups and Restorations.....	159
3.3.5.1 Creating a Manual Backup.....	160
3.3.5.2 Deleting a Manual Backup.....	161
3.3.5.3 Downloading a Full Backup.....	162
3.3.5.4 Checking and Exporting Backup Information.....	166

3.3.5.5 Restoring a FlexusRDS Instance.....	167
3.3.5.5.1 Restoring an Instance from Backups.....	167
3.3.5.5.2 Restoring an Instance to a Point in Time.....	169
3.3.6 Parameters.....	171
3.3.6.1 Suggestions on Parameter Tuning.....	172
3.3.6.2 Modifying Instance Parameters.....	174
3.3.6.3 Export a Parameter List.....	176
3.3.7 Logs.....	176
3.3.7.1 Viewing and Downloading Error Logs.....	176
3.3.7.2 Viewing and Downloading Slow Query Logs.....	178
3.3.8 Interconnection with CTS.....	180
3.3.8.1 Key Operations Supported by CTS.....	180
3.3.8.2 Viewing Traces.....	181
3.3.9 Managing Tags.....	181
3.3.10 Managing Quotas.....	182
4 Change History.....	184

1 FlexusL

1.1 Purchase a FlexusL Instance

Procedure

1. Log in to the FlexusL console.
2. Click **Buy FlexusL**.
3. Specify parameters for the FlexusL instance.

Parameter	Description
Region	<p>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.</p> <p>NOTE By default, all FlexusL instances created by the same account in the same region are located in the same VPC. They can communicate with each other over a private network. FlexusL instances that are created by different accounts or located in different regions cannot communicate with each other over a private network. For details, see Resource Configuration for FlexusL Instances.</p>

Parameter	Description
Image	<p>FlexusL provides OS images, application images, and private images for you to choose from.</p> <p>You need to learn about the constraints and usage of private images by referring to Managing Private Images before using them.</p> <p>NOTICE</p> <ul style="list-style-type: none"> The purchased FlexusL instance and the selected private image must be in the same region. For example, if you intend to purchase an instance in the AP-Singapore region, you can only select private images in the AP-Singapore region. To use an image in another region, replicate that image to the current region first by referring to Replicating Images Across Regions. If the message "This image has no password reset plug-in installed or onekey_resetpasswd tagged." is displayed when you use a private image to create a FlexusL instance or change the OS, resolve this issue by referring to What Should I Do If a Private Image Cannot Be Used to Create a FlexusL Instance or Change the OS of an Instance Because the Password Reset Plug-in Is Not Installed on the Image or the Image's onekey_resetpasswd Tag Is Missing?
Instance specifications	<p>You can select instance specifications based on your service requirements. Outbound traffic exceeding the traffic package is billed. For billing details, see Billing.</p> <p>NOTE</p> <p>If you use a private image, ensure that the image specifications are appropriate for creating this instance, or the instance creation or start may fail.</p>
(Optional) Instance name	<p>You can customize your instance name.</p> <p>If this parameter is left blank, the instance name is in the default format: image name-region-random number. In a batch creation, a hyphen followed by an incremental number is added to the end of each instance name by default.</p>
(Optional) Associated service resources	<p>You can associate the following service resources with your FlexusL instance as needed: data disks (EVS), host security (HSS basic edition), and cloud backup vaults (CBR).</p> <p>NOTE</p> <p>If you do not select Data Disk (EVS) during the purchase process, you can purchase it afterwards at the same price.</p>

Parameter	Description
Required duration	<p>The minimum duration of a purchase is one month and the maximum duration is three years.</p> <p>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.</p> <ul style="list-style-type: none">• Monthly subscription: auto-renews for 1 month every time• Yearly subscription: auto-renews for 1 year every time <p>For details about auto-renewal, see Auto-Renewal Rules.</p>
Quantity	Set the number of FlexusL instances to be purchased.

4. Click **Buy Now**.
On the displayed page, confirm the order details, read and select the agreement, and click **Submit**.
5. Select a payment method and complete the payment.
6. Go back to the FlexusL console and view the purchased FlexusL instance.

Follow-Up Operations

- When a FlexusL instance is being created, the initial password for logging in to the server is not set by default. [Set a password](#) first and then [log in to the FlexusL instance](#).
- If you select an application image when creating a FlexusL instance, you can log in to the visual dashboard of the image application for quick configuration. For details, see [Best Practices for FlexusL](#).
- If you select an OS image when creating a FlexusL instance, you need to set up an environment by yourself. You can see [Creating an Nginx Server Using the CentOS Image](#) or [Setting Up Websites](#) for reference.

NOTE

When you set up the environment by referring to [Setting Up Websites](#), ensure that the OS image version used by the FlexusL instance is the same as that in the tutorial to prevent command execution failures caused by version incompatibility.

1.2 Remotely Logging In to a FlexusL Instance Server

1.2.1 Overview

This section describes how to remotely log in to a FlexusL instance server. The login methods vary depending on the instance OS.

Login Overview (Linux)

The login mode varies depending on the local OS. You can select the login mode best suited to your local OS.

Table 1-1 Linux instance login modes

Cloud OS	Local OS	Login Mode	Requirement
Linux	Windows	(Recommended) Use CloudShell provided on the management console. Logging In to a FlexusL Instance Linux Server (Using CloudShell)	The FlexusL instance must have an EIP bound. NOTE By default, an EIP has been assigned to the FlexusL instance.
	Windows	Use a remote login tool, such as PuTTY or Xshell. The method is the same as logging in to an ECS. <ul style="list-style-type: none"> Using a password: Remotely Logging In to a Linux ECS (Using an SSH Password) Using a key pair: Remotely Logging In to a Linux ECS (Using an SSH Key Pair) 	
	Linux	Use commands. The method is the same as logging in to an ECS. <ul style="list-style-type: none"> Using a password: Remotely Logging In to a Linux ECS (Using an SSH Password) Using a key pair: Remotely Logging In to a Linux ECS (Using an SSH Key Pair) 	
	Mobile terminal	Use an SSH client tool, such as Termius or JuiceSSH. The method is the same as logging in to an ECS. Remotely Logging In to a Linux ECS (from a Mobile Terminal)	
	macOS	Use the terminal included in the macOS. The method is the same as logging in to an ECS. Remotely Logging In to a Linux ECS (from a macOS Server)	

Cloud OS	Local OS	Login Mode	Requirement
	Windows	Use the remote login function (VNC) available on the management console. For details, see Remotely Logging In to a FlexusL Instance Server (Using VNC) .	No EIPs are required.

Login Overview (Windows)

The login mode varies depending on the local OS. You can select the login mode best suited to your local OS.

Table 1-2 Windows instance login modes

Cloud OS	Local OS	Login Mode	Requirement
Windows	Windows	Use MSTSC. The method is the same as logging in to an ECS. Remotely Logging In to a Windows ECS (Using MSTSC)	The FlexusL instance must have an EIP bound. NOTE By default, an EIP has been assigned to the FlexusL instance.
	Linux	Install a remote connection tool, such as rdesktop. The method is the same as logging in to an ECS. Remotely Logging In to a Windows ECS (from a Linux Computer)	
	macOS	Install a remote connection tool, such as Microsoft Remote Desktop for Mac. The method is the same as logging in to an ECS. Remotely Logging In to a Windows ECS (from a macOS Server)	
	Mobile terminal	Install a remote connection tool, such as Microsoft Remote Desktop. The method is the same as logging in to an ECS. Remotely Logging In to a Windows ECS (from a Mobile Terminal)	

Cloud OS	Local OS	Login Mode	Requirement
	Windows	Use the remote login function (VNC) available on the management console. For details, see Remotely Logging In to a FlexusL Instance Server (Using VNC) .	No EIPs are required.

1.2.2 Remotely Logging In to a FlexusL Instance Server (Using VNC)


Scenarios

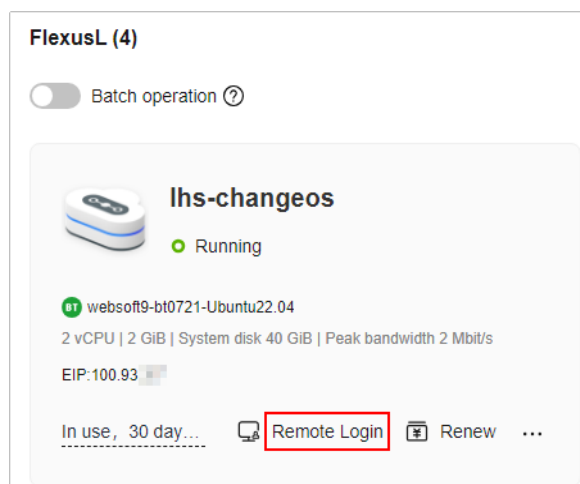
This section describes how to use VNC provided on the console to log in to a cloud server.

Notes and Constraints

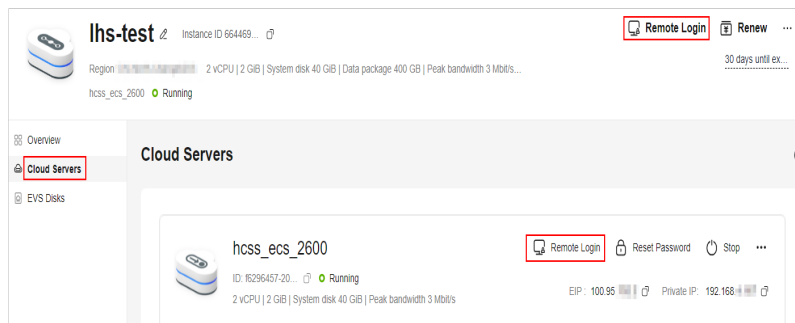
- You can only log in to a cloud server in the **Running** state.
- FlexusL instance servers do not have login passwords by default. When you log in to the server for the first time, [set a password](#).

Procedure

- Log in to the FlexusL console.
- Log in to a cloud server using any of the following methods.
 - In the **FlexusL** area, locate the target instance and click  **Remote Login**.



- Locate the target instance and click  **Remote Login** in the upper right corner.
- Locate the target instance, click **Cloud Servers** in the navigation pane on the left, and click  **Remote Login**.

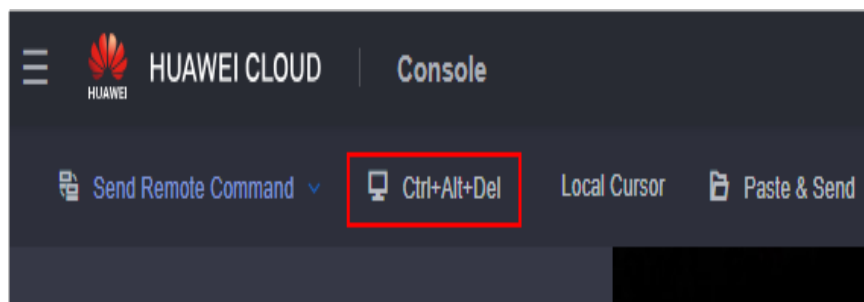


3. Log in to the FlexusL instance following the instructions.

For system security, the password you are entering is hidden by default. After you enter the correct password and press **Enter**, you can successfully log in to the server.

- For Windows: Click **Ctrl+Alt+Del** to unlock the desktop and enter the password.

The default username is **Administrator**.



- For Linux: Enter the username and password following the instructions. The default username is **root**.

```
Ubuntu 20.04.4 LTS smb-ecs-8e40 tty1
smb-ecs-8e40 login: root
Password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-100-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage
```

1.2.3 Logging In to a FlexusL Instance Linux Server (Using CloudShell)

Scenarios

This section describes how to use CloudShell to log in to a Linux cloud server. After login, if you need to use the copy-and-paste function provided by CloudShell, see [Common CloudShell Operations](#).

Prerequisites

- The status of the FlexusL instance must be **Running**.
- You have obtained the login username and password. If you have forgotten the password, [reset the password](#).

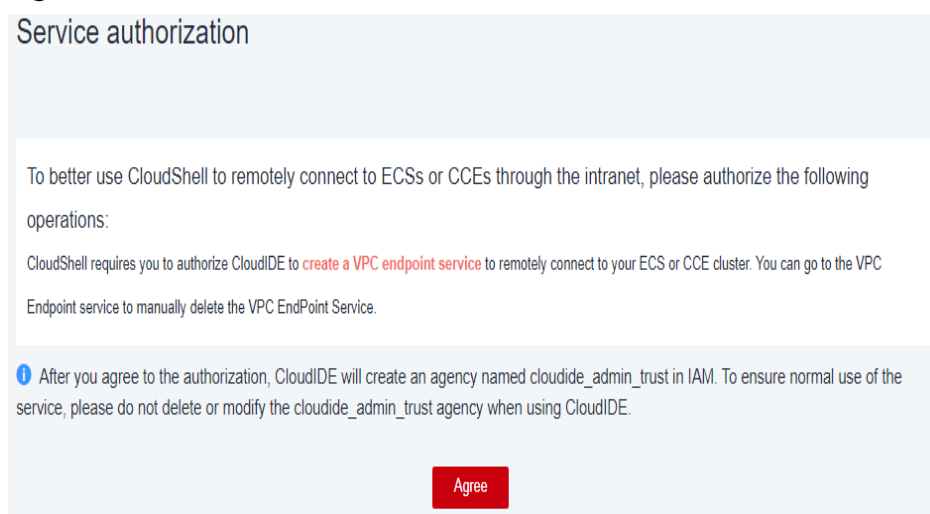
- The login port (port 22 by default) has been allowed by security group rules. For details about how to configure security group rules, see [Configuring Security Group Rules](#).

If a different port is required, you can use the default port to log in to the cloud server and then [change the port number](#).

- You can use CloudShell to connect to the cloud server through a public or private network. When you choose to connect through a private network, service authorization is required.
 - If the **Service authorization** page is displayed, it means you have the Security Administrator permissions. Click **Agree**.

The service authorization takes effect at the region level and is required only when you use CloudShell for the first time in a specific region.

Figure 1-1 Service authorization



- If you do not have the Security Administrator permissions, a page will be displayed, requiring you to contact the administrator to assign permissions to you.


Perform the following steps to assign permissions:

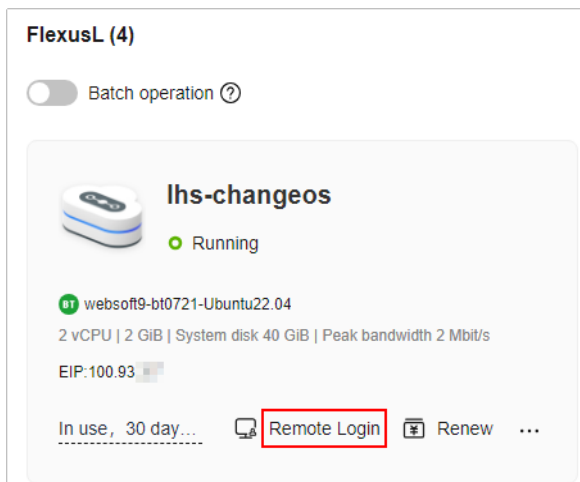
- i. Create a user group and assign the Security Administrator permissions to the user group. For details, see [Creating a User Group and Assigning Permissions](#).
- ii. Add the user to the user group. For details, see [Adding Users to or Removing Users from a User Group](#).

NOTE

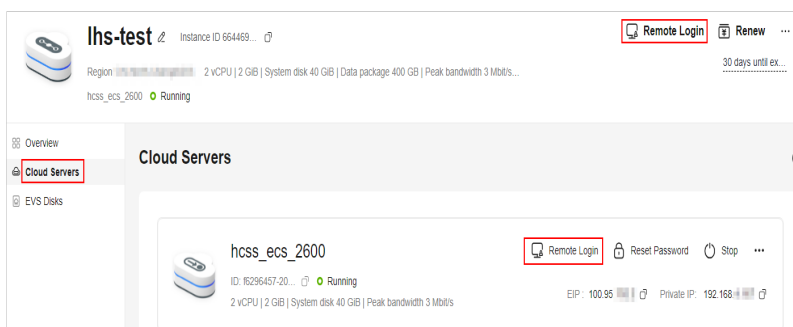
When you use CloudShell to remotely connect to the cloud server through a public network, service authorization is not required.

Procedure

1. Log in to the FlexusL console.
2. Log in to a cloud server using any of the following methods.
 - In the **FlexusL** area, locate the target instance and click  **Remote Login**.



- Locate the target instance and click **Remote Login** in the upper right corner.
- Locate the target instance, click **Cloud Servers** in the navigation pane on the left, and click **Remote Login**.



- In the displayed dialog box, click **Log In via CloudShell** in the **CloudShell Login** area.
- On the CloudShell page, configure information required for logging in to the FlexusL instance server.

When you log in for the first time, the CloudShell configuration wizard is displayed by default. Enter the parameters required for logging in to the cloud server.

Retain the default values of **Region** and **ECS**. Select either the EIP or the private IP address to log in.

- Using the EIP
 - Configure parameters for logging in to the cloud server.

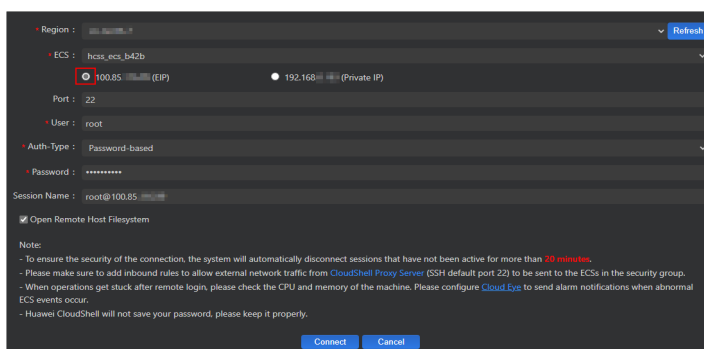


Table 1-3 Parameters for logging in to the cloud server

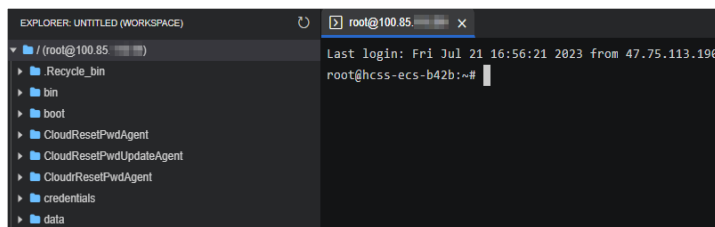
Parameter	Description
Port	Connection port, which is 22 by default. Ensure that the login port (port 22 by default) has been allowed by security group rules. For details about how to configure security group rules, see Configuring Security Group Rules .
User	Username for logging in to the cloud server, which is root by default.
Auth-Type	Select Password-based and enter the password for logging in to the cloud server. If you have not set the password or forgot the password, reset it .
Session Name	The default format is <i>Username@IP address</i> . You can change it as needed.

ii. Click **Connect**.

If a message is displayed indicating that the authentication fails, the possible cause is that the login password is not set or incorrect. [Reset the password](#) and try again.

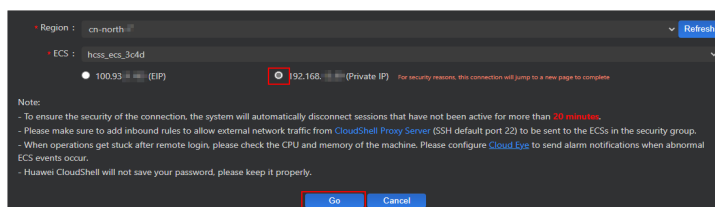
After the connection is successful, a figure similar to the following is displayed:

Figure 1-2 Successful login



– Using the private IP address

i. Click **Go**.



NOTE

If a message is displayed indicating that you do not have required permissions or an authorization is required, complete the service authorization as instructed in [#li16122162212615](#) first.

ii. On the new CloudShell configuration wizard page, configure parameters for logging in to the cloud server.

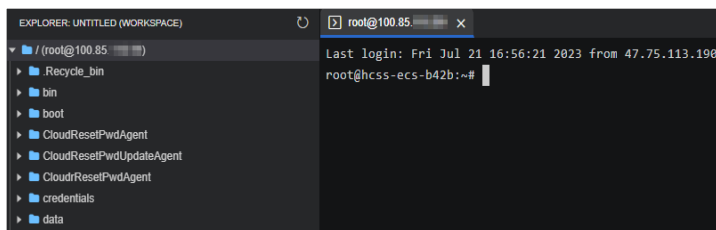
The configuration method using a private IP address is the same as that using an EIP. For details, see [Table 1-3](#).

iii. Click **Connect**.

If a message is displayed indicating that the authentication fails, the possible cause is that the login password is not set or incorrect. [Reset the password](#) and try again.

After the connection is successful, a figure similar to the following is displayed:

Figure 1-3 Successful login



1.3 Managing FlexusL Instances

1.3.1 Upgrading a FlexusL Instance

Scenarios

If the vCPUs, memory, system disk capacity, peak bandwidth, or data package of your FlexusL instance cannot meet your service requirements, you can upgrade the instance.

When you upgrade a FlexusL instance, the vCPUs, memory, system disk capacity, peak bandwidth, and data package packed into the instance are upgraded together to new specifications not lower than the current ones. For example, the following upgrade is not supported because the target peak bandwidth and data package are lower than the current ones.

Table 1-4 Unsupported upgrade

Instance Specifications	vCPUs Memory	System Disk	Peak Bandwidth	Data Package
Current	2 vCPUs 8 GiB	120 GiB	10 Mbit/s	2,000 GB
New	4 vCPUs 8 GiB	180 GiB	6 Mbit/s	1,200 GB

Constraints

- Resources (vCPUs, memory, data package, peak bandwidth, and system disk capacity) included in a FlexusL instance cannot be upgraded separately. They must be upgraded together.
- Instance specifications can only be upgraded, not downgraded. Upgraded instance specifications cannot be downgraded either.

Billing

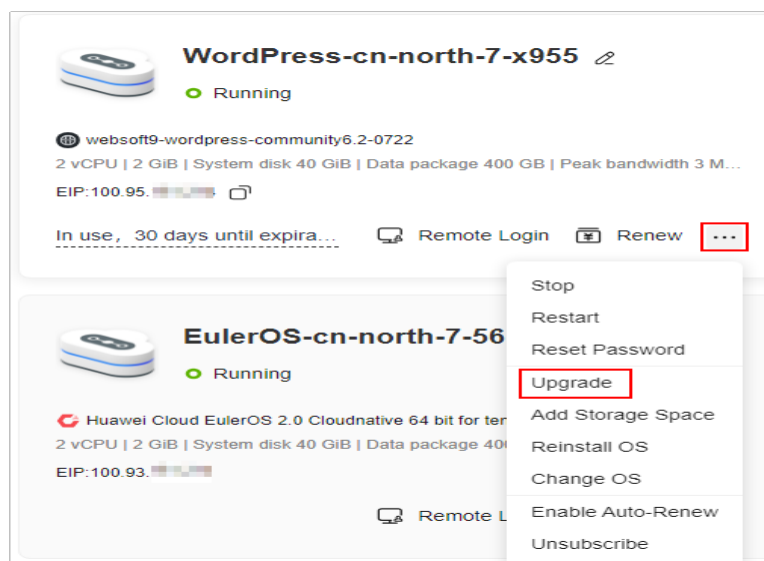
When upgrading specifications, you need to pay the difference in price. For details, see [Specifications Upgrade](#).

Preparations

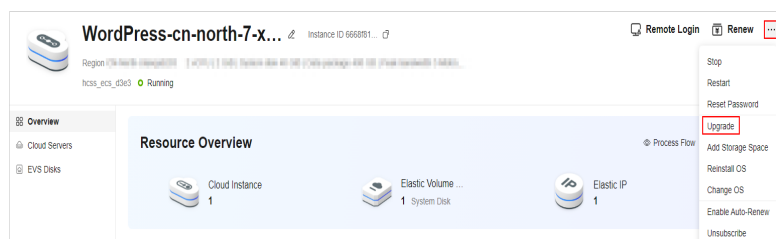
An upgrade failure may result in lost server data. You are advised to back up the data using CBR before you continue. For details, see [Method 2: Manual Backup](#).

Procedure

1. Log in to the FlexusL console.
2. Upgrading the FlexusL instances using any of the following methods.
 - Locate the target FlexusL instance, choose **...** > **Upgrade**.



- On the **Flexus L Instance** page, click the target instance name. On the displayed page, choose **...** > **Upgrade** in the upper right corner.



3. Select desired instance specifications on the displayed page. Grayed-out specifications are not supported for the upgrade.

Before upgrading specifications, stop the server first or select **Stop server** on the **Instance Upgrade** page.

4. Read and agree to the agreement, click **Submit**, and complete the payment.
5. Wait until the upgrade is complete and check whether the specifications are upgraded.

1.3.2 Searching for a FlexusL Instance

Scenario

After purchasing a FlexusL instance, you can use the search function on the management console to search for FlexusL instances quickly. You can directly enter an instance name without selecting a property in the search box and the system automatically matches the property type for search. Alternatively, you can manually select properties and enter or select property values for search.

Properties and Values

You can search for instances using any of the following properties: instance name, instance ID, EIP, server ID, and creation time. The value of a property is the property value.

Figure 1-4 Property and value

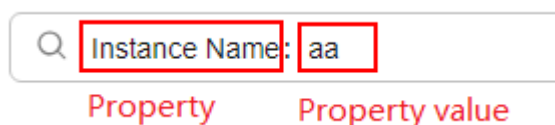



Table 1-5 describes each property.

Table 1-5 Property description

Property	Description
Instance name	Name of a FlexusL instance.
Instance ID	ID of a FlexusL instance.
EIP	Public IP address of a FlexusL instance.

Property	Description
Server ID	<p>ID of the cloud server in a FlexusL instance. Figure 1-5 shows the instance ID and cloud server ID on the FlexusL console.</p> <p>Figure 1-5 Instance ID and cloud server ID</p>  <p>The screenshot shows the FlexusL console interface. At the top, the instance name 'wp-30048110-408-v2-f' is displayed. Below it, the 'FlexusL instance ID' is shown as 'Instance ID 661390...'. The instance is in a 'Running' state. In the left sidebar, the 'Cloud Servers' tab is selected. The main content area shows a 'Cloud Servers' section with a card for the server 'hcss_ecs_2256'. The 'Cloud server ID' is shown as 'ID: e9f18f1e-04a4-40...'. The server is also in a 'Running' state. The console includes navigation tabs for Overview, Cloud Servers, EVS Disks, Cloud Backup Vaults, and Host Security.</p>
Creation time	Time when a FlexusL instance was created.

Constraints

- Only the instance name property supports fuzzy search, which means you can enter a part of a property value. Other properties (instance ID, EIP, server ID, and creation time) only support exact search, which means you must enter a complete property value.
- You cannot search for multiple instance names at the same time.

Procedure

In the search box, you can directly enter an instance name without selecting a property and the system automatically matches the instance name. For example, if you enter **aa** in the search box, the system will search for FlexusL instances whose names contain **aa**.

NOTE

Only the instance name property supports direct search in the search box. You do not need to select a property only when you search by instance name.

You can also manually select one or more properties and enter or select property values.

- Example 1: Searching by a single property with a single value
 - a. In the search box, select a property and select or enter a property value. For example, select the EIP property and enter **1.1.1.1** to search for the FlexusL instance whose EIP is 1.1.1.1.

- b. Press **Enter** to search.

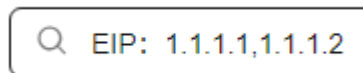


- Example 2: Searching by a single property with multiple values

You can select the same property for multiple times and enter or select property values. Alternatively, you can select a property, enter multiple property values and separate them with commas (,). Multiple property values of a single property are in OR relationship.

- a. Select a property from the search box, enter multiple property values, and separate them with commas (,).

For example, select the EIP property and enter **1.1.1.1,1.1.1.2** to search for the FlexusL instances whose EIP is 1.1.1.1 or 1.1.1.2.



- b. Press **Enter** to search.

You can find that the search results are the same as those searched by selecting one property and multiple property values.



- Example 3: Searching by multiple properties with multiple values

You can search by multiple properties and the properties are in AND relationship.

- a. In the search box, select a property and select or enter a property value, and press **Enter**.

For example, select the instance name property and enter **aa**.

- b. Add another property and value, and press **Enter**.

For example, select the creation time property and select a start date and end date. Then the FlexusL instances whose names contain **aa** and created within the specified time range are displayed.

Q Instance Name : aa X Created: Please select Created to search

Enter at least one date.

Start Date

2024/01/01 00:00:00

End Date

2024/02/01 00:00:00

Confirm Cancel

1.3.3 Renewing a FlexusL Instance

1.3.3.1 Overview

When to Renew Subscriptions

If a yearly/monthly FlexusL instance is about to expire but you want to continue using it, you need to renew the FlexusL subscription within a specified period, or it will be automatically released, and data will be lost and cannot be restored.

Only yearly/monthly FlexusL subscriptions can be renewed. The traffic usage in excess of the data package does not need to be renewed. Just ensure that your account has a valid payment method configured or a top-up account with a sufficient balance.

If you renew the FlexusL instance before it expires, resources will be retained and you can continue using them.

Notes

- If a resource is renewed when it is in a **grace period or retention period**, the renewal for this resource starts from when the resource expired instead of the current time.
- An FlexusL instance is actually a package of resources. Resources in the package can only be renewed together, not separately.
- Unsubscribed or released resources are not renewable.
- Orders being processed are not renewable.

How to Renew Subscriptions

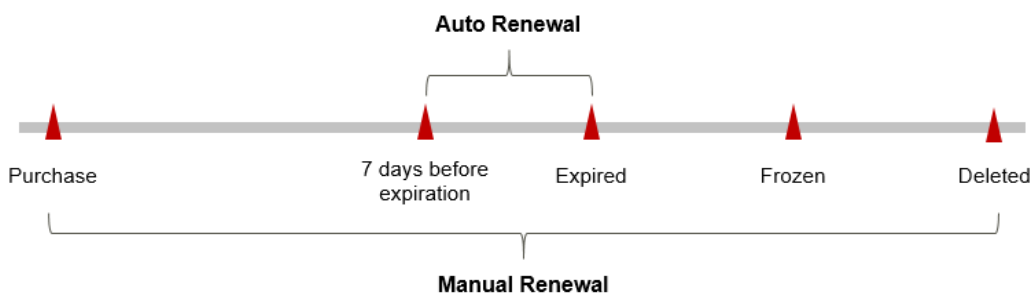
You can renew a yearly/monthly FlexusL instance manually or automatically.

Table 1-6 Renewing a yearly/monthly FlexusL instance

Method	Description
Manually Renewing FlexusL Instances	You can renew a yearly/monthly FlexusL instance on the console anytime before it is automatically deleted.
Auto-renewing a FlexusL Instance	You can enable auto-renew to automatically renew the FlexusL instance before it expires. This prevents resources from being deleted in case you forget to renew a subscription.

You can select a method to renew a yearly/monthly FlexusL instance based on the phase it is currently in.

Figure 1-6 Selecting a renewal method based on the FlexusL instance's current phase



- A FlexusL instance is in the **Running** state after it is provisioned.
- When the FlexusL subscription expires, the status will change from **Running** to **Expired**.
- If an expired FlexusL instance is not renewed, it enters a grace period. If it is not renewed by the time the grace period expires, it will be frozen and enter a retention period.
- If you do not renew the subscription before the retention period expires, your resources will be automatically deleted.

You can enable auto-renewal anytime before a FlexusL instance expires. By default, the system will make the first attempt to charge your account for the renewal at 03:00, seven days before the expiry date. If this attempt fails, it will make another attempt at 03:00 every day until the subscription is renewed or expires. You can change the auto-payment date for renewal as required.

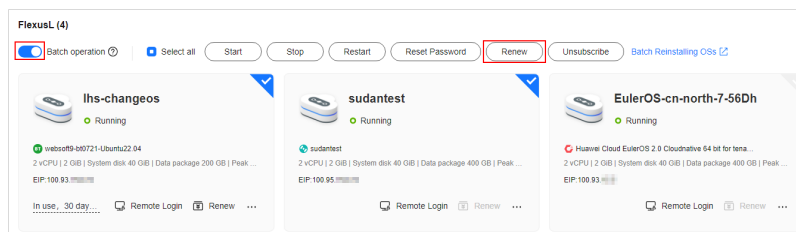
1.3.3.2 Manually Renewing FlexusL Instances

You can renew a yearly/monthly FlexusL instance anytime on the console before it is automatically deleted. This section describes how to manually renew a FlexusL instance. You can manually renew FlexusL instances in a batch on the FlexusL console or in Billing Center.

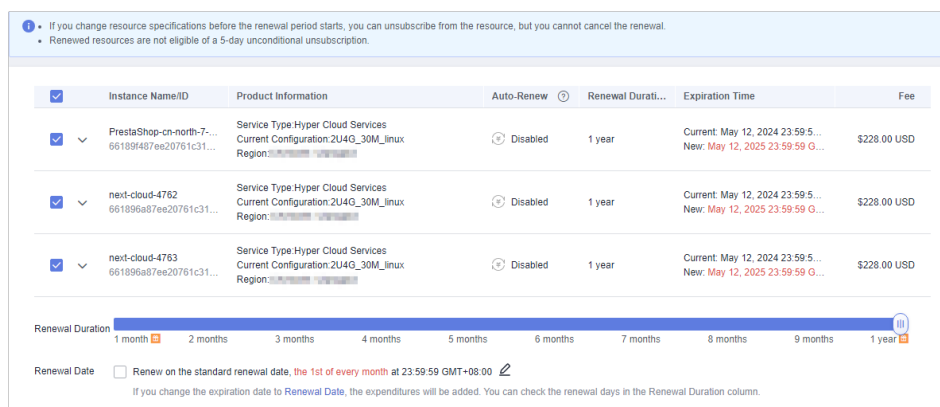
Batch Renewing FlexusL Instances on the Console

1. Log in to the FlexusL console.
2. Enable **Batch operation**, select the FlexusL instances to be renewed, and click **Renew**.

You can also use this method to renew just one FlexusL instance.



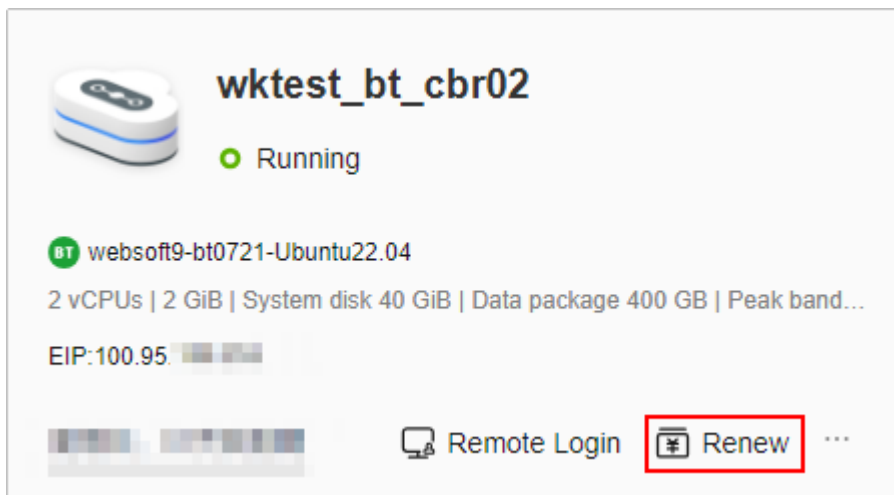
3. View the FlexusL instances to be renewed and click **OK**.
4. Set the renewal configurations, confirm the expected expiration date and price and click **Pay**.



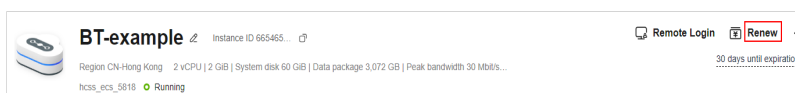
- Select a renewal duration.
 - Select **Renew on the standard renewal date**. For details, see [Setting the Same Renewal Day for Yearly/Monthly Resources](#).
5. Select a payment method and complete the payment.
Once the order is paid for, the renewal is complete.

Renewing a Single FlexusL Instance on the Console

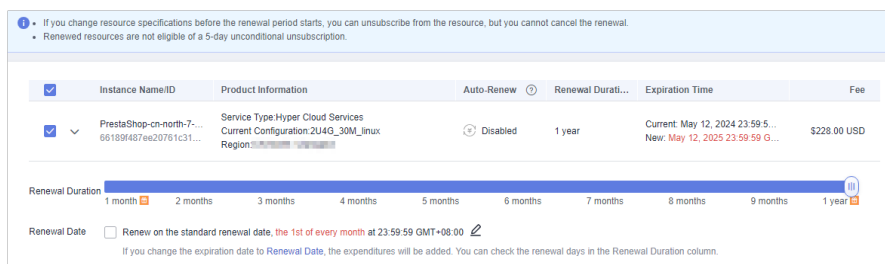
1. Log in to the FlexusL console.
2. Renew a FlexusL instance in either of the following two ways:
 - Method 1: Locate the target instance and click **Renew**.



- Method 2: Click the target instance name. On the displayed page, click **Renew** in the upper right corner.



3. Set the renewal configurations, confirm the expected expiration date and price and click **Pay**.



- Select a renewal duration.
- Select **Renew on the standard renewal date**. For details, see [Setting the Same Renewal Day for Yearly/Monthly Resources](#).

4. Select a payment method and complete the payment.

Once the order is paid for, the renewal is complete.

Renewing FlexusL Instances in Billing Center

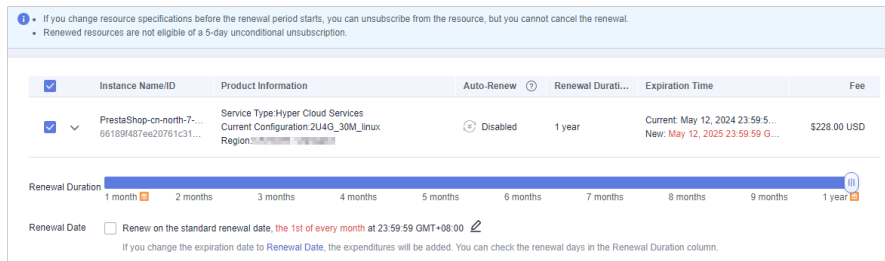
1. Log in to the FlexusL console.
2. In the upper-right corner of the console, choose **Billing > Renewal**.
3. Set the search criteria.

On the **Manual Renewals**, **Auto Renewals**, **Pay-per-Use After Expiration**, and **Renewals Canceled** tabs, you can view the resources to be renewed.

You can move all resources that need to be manually renewed to the **Manual Renewals** tab. For details, see [Enabling Manual Renewal](#).

4. Manually renew resources.
 - Individual renewal: Click **Renew** in the **Operation** column for the desired resource.

- Batch renewal: Check the boxes for the desired resources, and click **Batch Renew** in the upper left corner.
5. Set the renewal configurations, confirm the expected expiration date and price and click **Pay**.



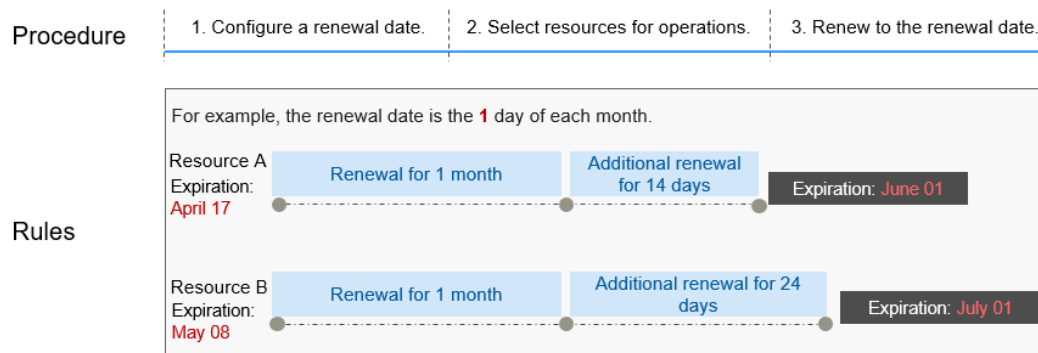
- Select a renewal duration.
 - Select **Renew on the standard renewal date**. For details, see [Setting the Same Renewal Day for Yearly/Monthly Resources](#).
6. Select a payment method and make your payment. Once the order is paid for, the renewal is complete.

Setting the Same Renewal Day for Yearly/Monthly Resources

If the FlexusL instances have different expiry dates, you can set the same renewal day to make it easier to manage renewals.

In [Figure 1-7](#), a user sets the same renewal day for two resources that will expire at different dates.

Figure 1-7 Setting the same renewal day for resources with different expiry dates



For details, see [Setting a Renewal Date](#).

1.3.3.3 Auto-renewing a FlexusL Instance

Auto-renew can prevent FlexusL instances from being automatically deleted if you forget to manually renew them. The auto-renewal rules are as follows:

- The first auto-renewal date is based on when the FlexusL instance expires and the billing cycle.
- FlexusL supports two auto-renew periods:
 - **Enabling Auto-Renew During Purchase**: Monthly subscriptions renew each month, and yearly subscriptions renew each year. For example, if

you set **Required Duration** to **3 months** and enable auto-renew, your subscription will be automatically renewed for one month before it expires.

- **Enabling Auto-Renew on the Renewals Page:** The auto-renew period is subject to the selected renewal period and auto-renew times. For example, if you set **New Auto-Renew Period** to **3 months** and **Auto-renewals** to **Unlimited**, your subscription will be automatically renewed for three months before it expires.
- You can enable auto-renew anytime before a subscription expires. By default, the system will make the first attempt to charge your account for the renewal at 03:00 seven days before the expiry date. If this attempt fails, it will make another attempt at 03:00 every day until the subscription is renewed or expires.
- After auto-renew is enabled, you can still renew your subscription manually if you want to. After a manual renewal is complete, auto-renewal is still valid, and the renewal expenditure will be deducted from your account seven days before the new expiry date.
- By default, the renewal expenditure is deducted from your account seven days before the new expiry date. You can change this auto-renew payment date as required.

For more information about auto-renewal rules, see [Auto-Renewal Rules](#).

Prerequisites

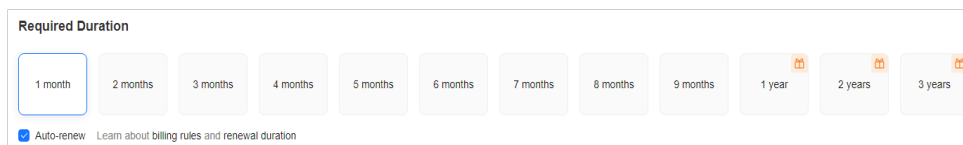
The yearly/monthly FlexusL instance has not expired.

Enabling Auto-Renew During Purchase

You can enable auto-renew on the purchase page, as shown in [Figure 1-8](#). For details, see [Purchasing a FlexusL Instance](#).

If you select **Auto renew**, monthly subscription is auto-renewed for one month every time and yearly subscription is auto-renewed for one year every time. For example, if you set **Required Duration** to **3 months** and enable auto-renew, your subscription will be automatically renewed for one month before it expires.

Figure 1-8 Enabling auto-renew



Enabling Auto-Renew on the FlexusL Console

1. Log in to the FlexusL console.
2. Enable auto-renew in either of the following ways:
 - a. Locate the target instance and choose ******* > **Enable Auto-Renew** in the instance card.

- b. Click the target instance name. On the displayed page, choose **...** > **Enable Auto-Renew** in the upper right corner.

NOTE

After auto-renew is enabled, you can choose **...** > **Modify Auto-Renew** to modify the auto-renew rules.

3. Select a renewal period, specify the auto-renew times, and click **Pay**.

If auto-renew is enabled on the **Renewals** page, the auto-renew period is subject to the selected renewal period and auto-renew times. For example, if you set **New Auto-Renew Period** to **3 months** and **Auto-renewals** to **Unlimited**, your subscription will be automatically renewed for three months before it expires.

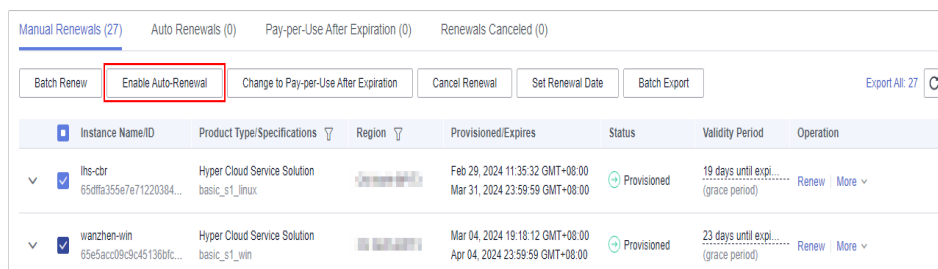
NOTE

- When the number of times a resource has been auto-renewed for reaches the preset value, the resource will be automatically changed to manual renewal upon expiration.
- Manual renewal does not affect the number of remaining auto-renew times.

Enabling Auto-Renew on the Renewals Page

1. Log in to the FlexusL console.
2. In the upper-right corner of the console, choose **Billing** > **Renewal**.
 - You can filter resources by the expiration time or status.
 - You can view the resources for which auto-renew has been enabled on the **Auto Renewals** tab.
 - You can enable auto-renew for resources on the **Manual Renewals**, **Pay-per-Use After Expiration**, and **Renewals Canceled** tabs.
3. Enable auto-renew for yearly/monthly resources.
 - Enabling auto-renewal for a single resource: Select the resource for which you want to enable auto-renew and click **Enable Auto-Renew** in the **Operation** column.
 - Enabling auto-renew for multiple resources at a time: Select the resources for which you want to enable auto-renew and click **Enable Auto-Renew** above the list.

Figure 1-9 Enabling auto-renew for multiple resources



Instance Name/ID	Product Type/Specifications	Region	Provisioned/Expires	Status	Validity Period	Operation
<input checked="" type="checkbox"/> lhc-ctr 65dfda355e7e71220384...	Hyper Cloud Service Solution basic_s1_linux	...	Feb 29, 2024 11:35:32 GMT+08:00 Mar 31, 2024 23:59:59 GMT+08:00	Provisioned	19 days until expt... (grace period)	Renew More ▾
<input checked="" type="checkbox"/> wanzhen-win 65e5acc09c9c451386fc...	Hyper Cloud Service Solution basic_s1_win	...	Mar 04, 2024 19:18:12 GMT+08:00 Apr 04, 2024 23:59:59 GMT+08:00	Provisioned	23 days until expt... (grace period)	Renew More ▾

4. Select a renewal period, specify the auto-renew times, and click **Pay**.

If auto-renew is enabled on the **Renewals** page, the auto-renew period is subject to the selected renewal period and auto-renew times. For example, if

you set **New Auto-Renew Period to 3 months** and **Auto-renewals to Unlimited**, your subscription will be automatically renewed for three months before it expires.

NOTE

- When the number of times a resource has been auto-renewed for reaches the preset value, the resource will be automatically changed to manual renewal upon expiration.
- Manual renewal does not affect the number of remaining auto-renew times.

1.3.4 Unsubscribing from a FlexusL Instance

Unsubscription includes unsubscribing from resources and unsubscribing from renewal periods. After the unsubscription is successful, you will get a refund.

- Unsubscribing from resources: You can unsubscribe from FlexusL instances (including the renewal period) that are no longer needed. A FlexusL instance is actually a package of resources. If you unsubscribe from a FlexusL instance, all resources including the EVS disks, cloud backup vault, HSS, and EIP associated with the instance will be released and data cannot be recovered.
- Unsubscribing from a renewal period: If you have renewed a FlexusL instance, you can unsubscribe from the renewal period. When you unsubscribe from a renewal period, you can only unsubscribe from the renewal period that has not yet taken effect. To unsubscribe from the renewal period that has taken effect, you can only unsubscribe from the FlexusL instance.

Notes

- Before unsubscription, ensure that data on the cloud resources to be unsubscribed from has been backed up or migrated. After unsubscription, resources will be deleted and data cannot be recovered. Exercise caution during unsubscription.
- If no more than five days have elapsed after you purchased a resource and the number of your historical unsubscriptions in that year is no more than 10, you can get a full refund unconditionally. The 5-day unconditional full refund does not apply to inactive resources or resources in a renewal period.
- If an order is paid using the Huawei Cloud account balance or a third-party online payment platform (such as Alipay, WeChat, or e-banking), the refund will be returned to your Huawei Cloud account balance.

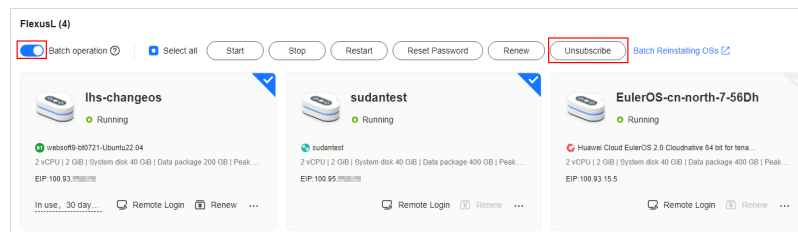
Constraints

- Newly purchased FlexusL instances cannot be unsubscribed from immediately. Try later.
- FlexusL instances that are in the **grace period or retention period** due to arrears cannot be unsubscribed from. To unsubscribe from such instances, pay off the arrears first. If you still do not pay off the arrears after the retention period has ended, all of your resources will be released.
- FlexusL instances that are frozen due to illegal issues cannot be unsubscribed from.

Batch Unsubscribing from FlexusL Instances

1. Log in to the FlexusL console.
2. Enable **Batch operation**, select the FlexusL instances to be unsubscribed, and click **Unsubscribe**.

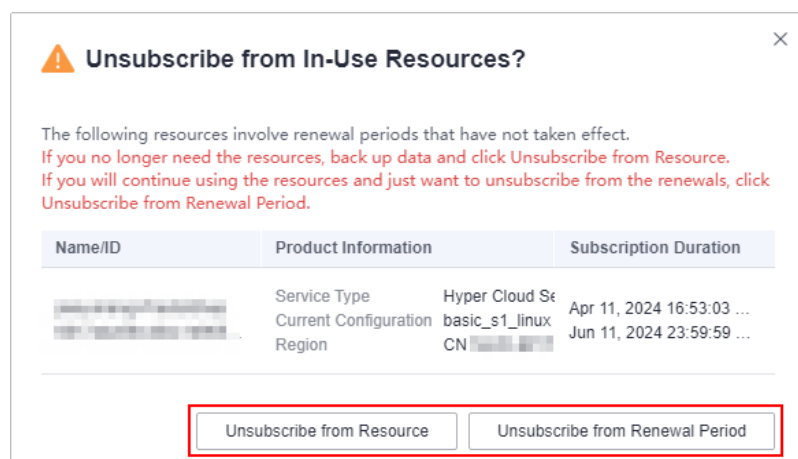
You can also use this method to unsubscribe just one FlexusL instance.



3. View the FlexusL instances to be unsubscribed and click **OK**.
4. (Optional) Unsubscribe from a resource or a renewal period.

You can unsubscribe from a renewal period only when your FlexusL instances have a renewal period.

- Unsubscribing from resources: You can unsubscribe from FlexusL instances (including the renewal period) that are no longer needed. A FlexusL instance is actually a package of resources. If you unsubscribe from a FlexusL instance, all resources including the EVS disks, cloud backup vault, HSS, and EIP associated with the instance will be released and data cannot be recovered.
- Unsubscribing from a renewal period: If you have renewed a FlexusL instance, you can unsubscribe from the renewal period. When you unsubscribe from a renewal period, you can only unsubscribe from the renewal period that has not yet taken effect. To unsubscribe from the renewal period that has taken effect, you can only unsubscribe from the FlexusL instance.

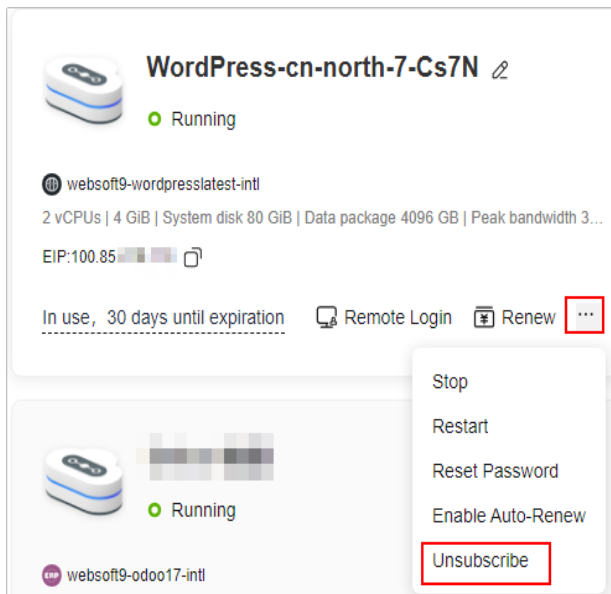


5. Confirm the unsubscription details and click **Confirm**.

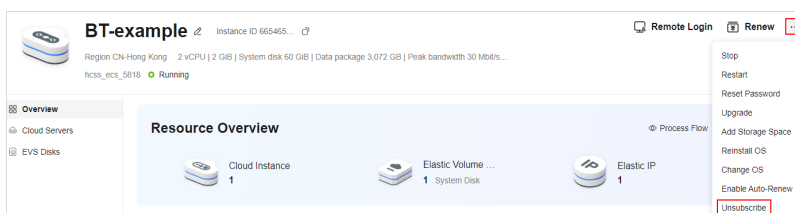
Unsubscribing from a Single FlexusL Instance

1. Log in to the FlexusL console.
2. Unsubscribe from a FlexusL instance using any of the following methods.

- Method 1: Locate the target instance and choose **...** > **Unsubscribe** in the instance card.



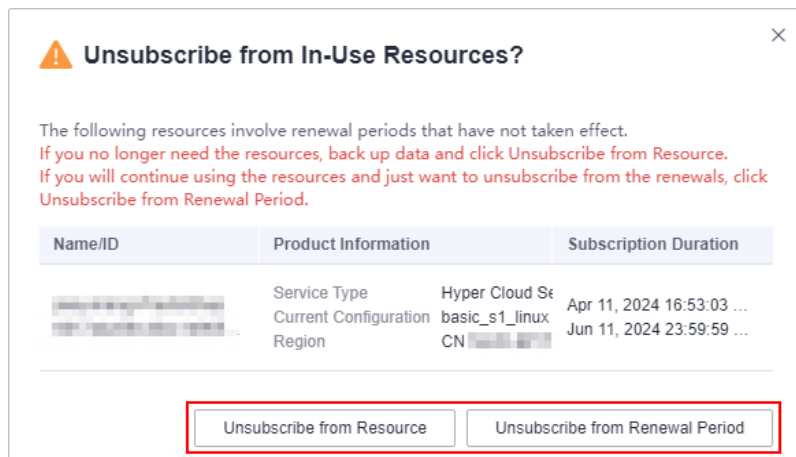
- Method 2: Click the target instance name. On the displayed page, choose **...** > **Unsubscribe** in the upper right corner.



3. (Optional) Unsubscribe from a resource or a renewal period.

You can unsubscribe from a renewal period only when your FlexusL instances have a renewal period.

- Unsubscribing from resources: You can unsubscribe from FlexusL instances (including the renewal period) that are no longer needed. A FlexusL instance is actually a package of resources. If you unsubscribe from a FlexusL instance, all resources including the EVS disks, cloud backup vault, HSS, and EIP associated with the instance will be released and data cannot be recovered.
- Unsubscribing from a renewal period: If you have renewed a FlexusL instance, you can unsubscribe from the renewal period. When you unsubscribe from a renewal period, you can only unsubscribe from the renewal period that has not yet taken effect. To unsubscribe from the renewal period that has taken effect, you can only unsubscribe from the FlexusL instance.



4. Confirm the unsubscription details and click **Confirm**.

1.4 Managing Cloud Servers

1.4.1 Managing an Instance Lifecycle

The FlexusL lifecycle refers to the entire journey a FlexusL instance goes through, from creation to deletion or unsubscription.

Instance Statuses

The following table lists all the statuses that a FlexusL instance may be in.

Status	Attribute	Description
Creating	Intermediate	The instance is being created. No operations can be performed on an instance in Creating state.
Running	Stable	The instance is running properly and can be accessed only when it is in this state.
Updating	Intermediate	The configuration of the instance is being modified, such as expanding the capacity or adding resources.
Restarting	Intermediate	The instance is being restarted on the console. No operations can be performed on an instance in Restarting state. If an instance has been in this state for a long time, an exception may occur.
Starting	Intermediate	The instance is being started on the console. No operations can be performed on an instance in Starting state. If an instance has been in this state for a long time, an exception may occur.
Stopping	Intermediate	The instance is being stopped on the console. No operations can be performed on an instance in Stopping state. If an instance has been in this state for a long time, an exception occurs.

Status	Attribute	Description
Stopped	Stable	The instance has been stopped on the console. A stopped instance cannot provide services.
Unsubscribing	Intermediate	The instance is being unsubscribed from. After unsubscription, resources will be released.
Frozen	Stable	The instance violates regulations or enters the retention period after it expires.
Unfreezing	Intermediate	<ul style="list-style-type: none">You can appeal for an instance that is frozen due to public security reasons or violation against regulations. After the appeal is approved, the instance is in Unfreezing state.An instance is frozen when it expires and enters the retention period. After you renew the subscription, the instance is in Unfreezing state. After being unfrozen, the instance can be used properly.
Abnormal	Faulty	The instance is faulty. No operations can be performed on an instance in Abnormal state. Contact customer service for assistance.

Manage Instances

- Purchasing an instance
 - You can purchase an FlexusL instance (see [Purchase a FlexusL Instance](#)) and specify your instance specifications during the purchase process. The instance is in **Creating** state when it is being created.
 - After the instance is created, its status becomes **Running**. For details, see [Remotely Logging In to a FlexusL Instance Server \(Using VNC\)](#).
- Restarting an instance
 - The instance status is **Restarting** when it is being restarted.
 - Some changes will be applied only after the instance is restarted. For example, the password change will be applied only after the instance is restarted.
 - Restarting an instance usually takes dozens of seconds to several minutes, depending on the instance configuration.
- Stopping an instance

If the instance is no longer used, you can stop it on the console. Stopped instances do not provide services.
- Renewing an instance

You can manually or automatically renew an instance after it expires. For details, see [Renewing a FlexusL Instance](#).
- Unsubscribing from an instance



If an instance has expired and is no longer needed, you can manually unsubscribe from it or wait for the system to automatically release it. For details, see [Unsubscribing from a FlexusL Instance](#).

1.4.2 Viewing Cloud Server Details

After purchasing a FlexusL instance, you can view and manage it on the FlexusL console. This section describes FlexusL instance details and related operations.

Procedure

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

Server Details	Description
Name/ID	Cloud server name or ID
Status	Server status. For details, see Instance Statuses .
Security	Servers scanned by HSS <ul style="list-style-type: none">• : No risks detected.• : Risks detected. You can view risk details on the console.
Specification	vCPUs, memory, system disk, and bandwidth of a server
IP address	Private IP or EIP of a server
Operation	Operations supported by a server

3. Click the server name to go to the server details page.
You can view server details on the **Overview**, **Domain Names**, **Security Groups**, **Disks**, and **Network Interfaces** tabs.

Tab	Description
Overview	On the Overview tab, you can view: <ul style="list-style-type: none">• Basic information: including the instance name, ID, region, and expiration time.• Configuration information: including the vCPU/memory, disk capacity and type, bandwidth, and image.• Network information: including the network interface name and IP (used for communication between instances), VPC, EIP (used for internet access), and security group.
Domain Names	On the Domain Names tab, you can: <ul style="list-style-type: none">• View domain names.• Add, resolve, disable, or delete a domain name. For details, see Managing Domain Names.

Tab	Description
Security Groups	On the Security Groups tab, you can: <ul style="list-style-type: none">• View inbound and outbound security group rules.• Change the security group. For details, see Changing a Security Group.• Configure security group rules. For details, see Configuring Security Group Rules.
Disks	On the Disks tab, you can view disk details, including the disk ID, mount point, capacity, and encryption status.
Network Interfaces	On the Network Interfaces tab, you can: <ul style="list-style-type: none">• View network interface details, including the ID, EIP, private IP address, security group, and MAC address.• Change the security group. For details, see Changing a Security Group.

1.4.3 Setting or Resetting a Password

You can set or reset the password for logging in to one or more cloud servers at a time.

- A FlexusL instance does not have an initial password. You need to set a password when you use the FlexusL instance for the first time.
- If the password is lost or expires, you can reset the password.

Constraints

- You can reset the password only when the server is in **Stopped** or **Running** state. If you reset the password when the server is in **Running** state, the password change will be applied only after the server is restarted.
- The one-click password reset plug-in must have been installed.

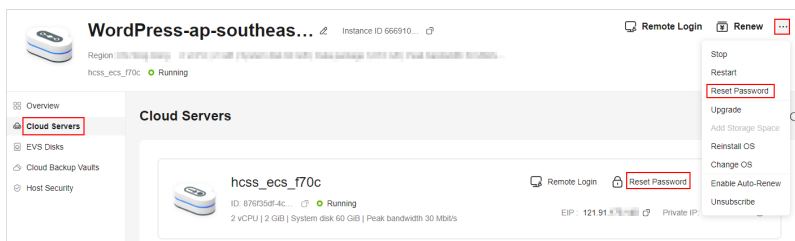
If a private Linux image is created from a server on another cloud platform or downloaded from a third party, the image may not have the password reset plug-in installed. Servers created from such images do not support password reset. For details about how to install the one-click password reset plug-in and reset the password, see [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?](#)

- Do not delete the password reset processes **CloudResetPwdAgent** and **CloudResetPwdUpdateAgent**, or the password reset will be unavailable.
- Ensure that DHCP is enabled in the VPC which the server belongs to.
- Ensure that the network is normal.

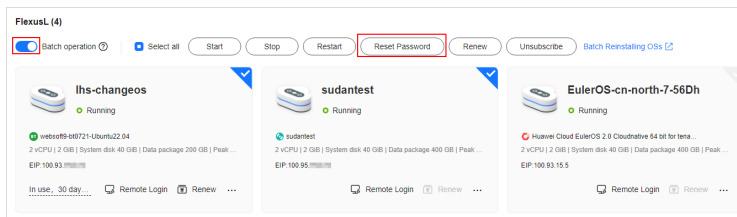
Procedure

1. Log in to the FlexusL console.

2. Reset the password for logging in to one or more servers.
 - Resetting the password for logging in to a server in any of the following ways:
 - In the **FlexusL** area, locate the target instance and choose **...** > **Reset Password**.
 - Click the target instance name. On the displayed page, choose **...** > **Reset Password** in the upper right corner.
 - Click the target instance name. In the left navigation pane, choose **Cloud Servers** and click **Reset Password** in the row containing the target server.

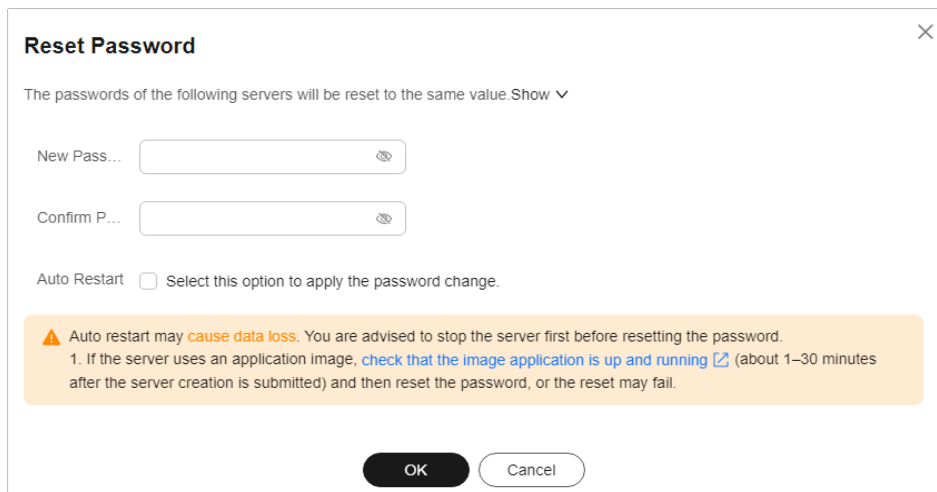


- Batch resetting the login passwords
Enable **Batch operation**, click **Select all** or select the instances for which you want to change the server login password, and click **Reset Password**. After the passwords are reset in a batch, the passwords for logging in to these instance servers are the same.



3. Set and confirm a new password as prompted.
If you reset the password for a running server, the password change is applied only after the next restart. Select **Auto Restart**.

Figure 1-10 Reset a password



- The new password must meet the password complexity requirements.
- Click **OK**.
- The password change will be applied after the server is restarted.

NOTE

- Do not reset the password repeatedly.
- Restarting an instance usually takes dozens of seconds to several minutes, depending on the instance configuration.

1.4.4 Reinstalling an OS

If the OS of a FlexusL instance is abnormal, reinstall the OS.

This section describes how to reinstall the OS of a FlexusL instance. For details about how to reinstall the OSs of multiple FlexusL instances in batches, see [Batch Reinstalling OSs](#).

Notes

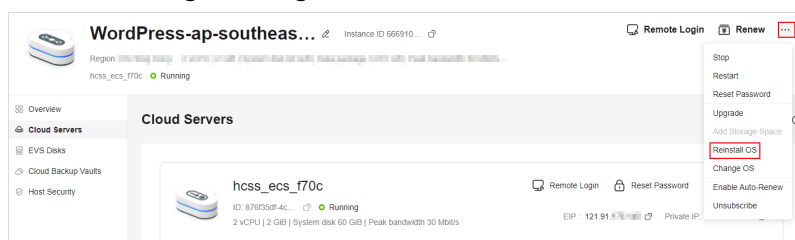
- After the OS is reinstalled, the IP address of the cloud server remains unchanged.
- Reinstalling the OS clears the data in all partitions, including the system partition, of the system disk. Back up data before reinstalling the OS.
- Reinstalling the OS does not affect data disks.
- Do not perform any operations on the cloud server immediately after its OS is reinstalled. Wait for several minutes until the system successfully injects the password or key, or the injection may fail, and the server cannot be logged in to.
- The server will automatically restart after the OS is reinstalled, and only custom settings (such as the DNS) will be reset.

Billing

OS reinstallation is free because the original image will be used.

Procedure

- Log in to the FlexusL console and click a resource card to go to the instance details page.
- Reinstall the OS using any of the following methods.
 - Method 1: Locate the target FlexusL instance and choose ******* > **Reinstall OS**.
 - Method 2: On the **Cloud Servers** page, choose ******* > **Reinstall OS** in the row containing the target cloud server.



- Method 3: On the **Cloud Servers** page, click the target server name. In the upper right corner of the displayed page, choose **...** > **Reinstall OS**.
3. Specify the parameters required for reinstalling the OS.
- Select **Stop server**. The server must be stopped before its OS can be reinstalled.
 - Set **Login Credentials**. The credentials are used for logging in to cloud servers. After the OS is reinstalled, the login password is cleared. Reset the password.
 - Read and agree to the agreement/disclaimer.

Reinstall OS

i OS reinstallation is free because the original image will be used.
An OS reinstallation has no impact on data disks, but all data on and all backups created for the system disk will be deleted. Back up data before you continue.
The server will automatically restart after the OS is reinstalled, and custom settings (such as the DNS) will be reset.

Current Configuration

Name	IP Address	Specifications	Image
hcsc_ecs_4a1a	192.168.1.1 (private)	2 vCPUs 2 GiB System disk 40 GiB	Windows Server 2019

Stop server (The server must be stopped before its OS can be reinstalled.)

Login Credentials

New Pass...

Confirm P...

I have read and agree to the [Image Disclaimer](#).

OK **Cancel**

4. Click **OK**.

After the OS is reinstalled, the cloud server will automatically restart. When the server status is **Running**, the OS reinstallation is complete.

1.4.5 Batch Reinstalling OSs

Scenarios

Huawei Cloud Operations Center (COC) allows you to reinstall the OSs of multiple FlexusL instances in batches on the COC console.

Notes

- After the OS is reinstalled, the IP address of the cloud server remains unchanged.
- Reinstalling the OS clears the data in all partitions, including the system partition, of the system disk. Back up data before reinstalling the OS.
- Reinstalling the OS does not affect data disks.

- Do not perform any operations on the cloud server immediately after its OS is reinstalled. Wait for several minutes until the system successfully injects the password or key, or the injection may fail, and the server cannot be logged in to.
- The server will automatically restart after the OS is reinstalled, and only custom settings (such as the DNS) will be reset.

Billing

OS reinstallation is free because the original image will be used.

Preparations

Before reinstall OSs, make the following preparations:

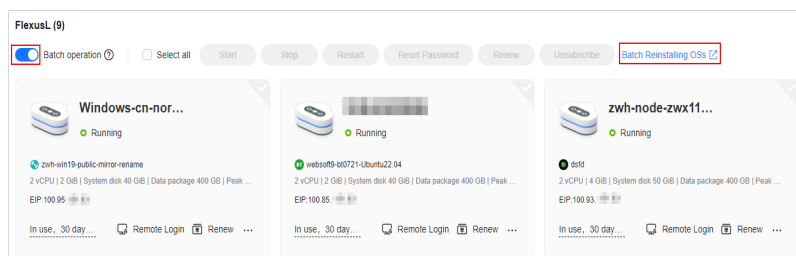
1. Prepare the COC FullAccess permissions.
 - If you are using a Huawei Cloud account, it has the COC FullAccess permissions by default. You can skip this step.
 - If you are an IAM user, a message is displayed, indicating that you do not have the required permissions. The account administrator needs to grant you the COC FullAccess permissions by doing the following:
 - i. Grant a user group the COC FullAccess permissions. For details, see [Creating a User Group and Assigning Permissions](#).
 - ii. Add the IAM user to the group. For details, see [Adding Users to a User Group](#).
2. Apply for the COC open beta testing (OBT).

COC is in the OBT phase. After you have been granted the COC FullAccess permissions, apply for the COC OBT.

Procedure

1. Log in to the FlexusL console, enable **Batch operation**, and click **Batch Reinstalling OSs** to go to the COC console.

You can also directly access the [COC](#) console. If a message is displayed indicating that you do not have the required permissions or need to apply for the OBT, perform the operations described in [Preparations](#) first.

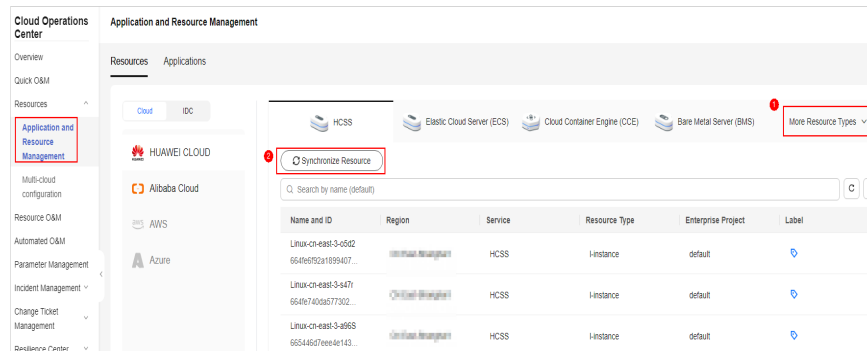


2. In the navigation pane, choose **Resources > Application and Resource Management**. On the **Resources** tab, choose **More Resource Types > Compute > FlexusL** and click **Synchronize Resource**.

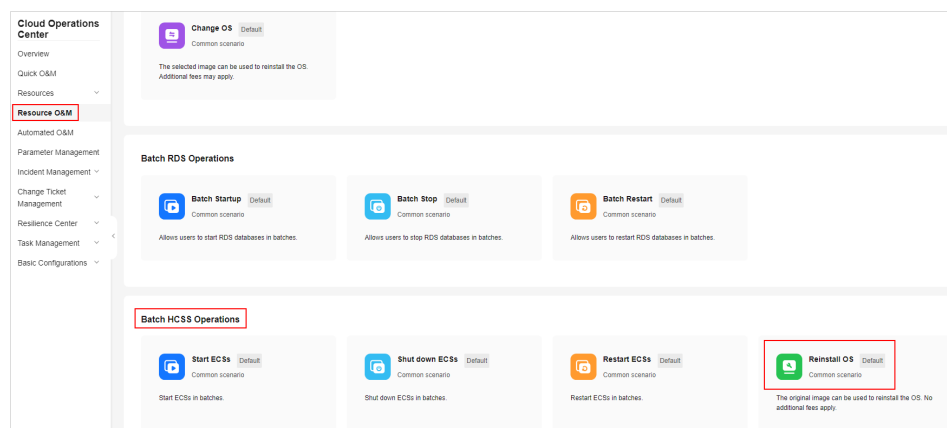
Before batch reinstalling OSs, you must synchronize FlexusL instance resources to COC. The COC obtains the synchronized resources and then can reinstall OSs for the FlexusL instances. Once new FlexusL instances are

created, you must synchronize their resources to the COC console so that you can reinstall OSs in batches on the COC console.

The resources synchronized to COC are all FlexusL instance resources created by your account in all regions.

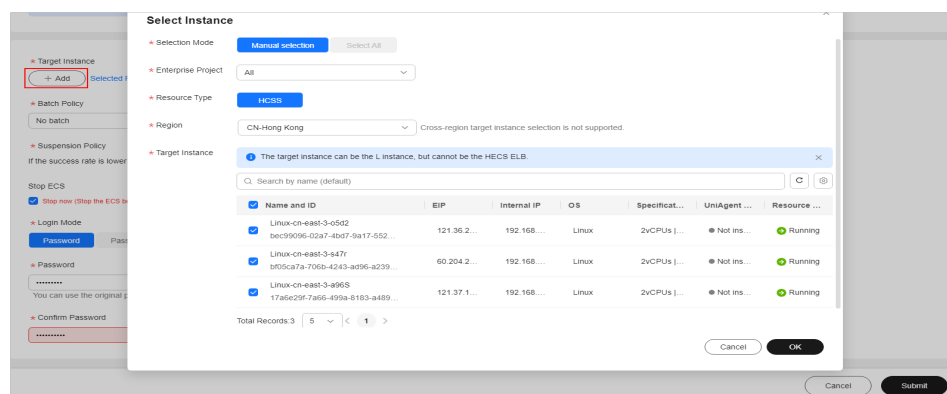


3. In the left navigation pane, choose **Resource O&M**. In the **Batch HCSS Operations** area, click **Reinstall OS**.



4. On the displayed page, configure parameters required for batch OS reinstallation.

Figure 1-11 Batch reinstalling OSs



Parameter	Description
Target Instance	<ul style="list-style-type: none">● Selection Mode: Manual selection (only this option supported)● Enterprise Project: All● Resource Type: HCSS, indicating that OSs are batch reinstalled for FlexusL instances● Region: Select the region where FlexusL instances are located. The instances must be in the same region. Batch OS reinstallation is not available for FlexusL instances in different regions.● Target Instance: Select the FlexusL instances whose OSs are to be reinstalled. If some FlexusL instances are missing in the list, synchronize resources first.
Batch Policy	<p>Select a batch policy based on your requirements.</p> <ul style="list-style-type: none">● Automatic: The selected FlexusL instances are automatically divided into multiple batches based on the preset rule.● Manual: You can manually create multiple batches and add FlexusL instances to each batch as required.● No batch: All selected FlexusL instances are in the same batch. <p>NOTE</p> <ul style="list-style-type: none">● If you select Automatic or Manual and multiple batches of OS reinstallation tasks are generated, the process will be suspended after each batch of tasks is executed. You need to manually continue the next batch. For details, see Related Operations.● If there are services running on your FlexusL instances, the No batch policy may affect your services. You are advised to select the automatic or manual batch policy.
Suspension Policy	<p>Determine the policy for suspending a task. You can set the success rate of OS reinstallation. When the success rate is lower than the specified value, the task status becomes abnormal and the task is suspended. The value is from 0 to 100 and can be accurate to one decimal place.</p> <p>Success rate = (Number of FlexusL instances whose OSs are successfully reinstalled/Total number of FlexusL instances) x 100%</p>
Stop ECS	<p>This option is displayed when there are FlexusL instances in Running state. Select Stop now.</p>
Login Mode	<ul style="list-style-type: none">● Password: Set a unified password for logging in to FlexusL instances whose OSs are to be installed.● Reset password: Reset the password when logging in to the FlexusL instances for the first time. <p>NOTE Currently, FlexusL instances do not support key pairs.</p>

- Click **Submit**. Confirm the information and click **OK** to start the OS reinstallation.

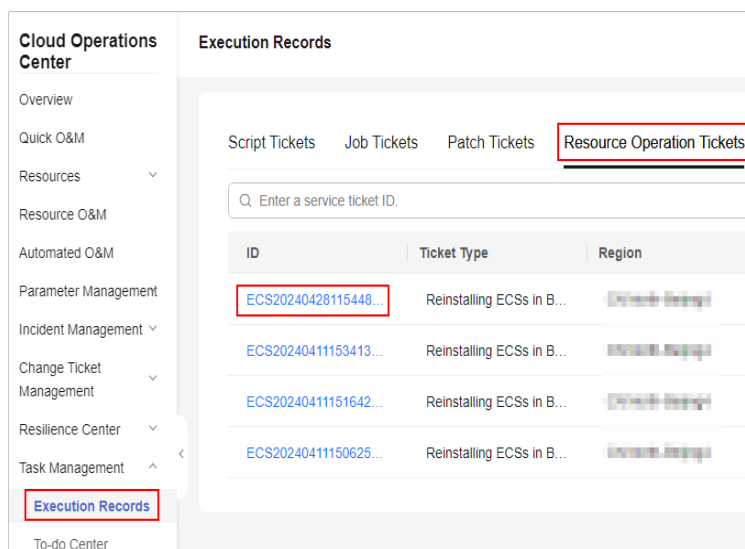
After the OS is reinstalled, the cloud server will automatically restart. When the server status is **Running**, the OS reinstallation is complete.

After the request is submitted, the system generates a service ticket and you will be automatically redirected to the [service ticket details page](#). You can also [view the service ticket details](#) later.

Related Operations

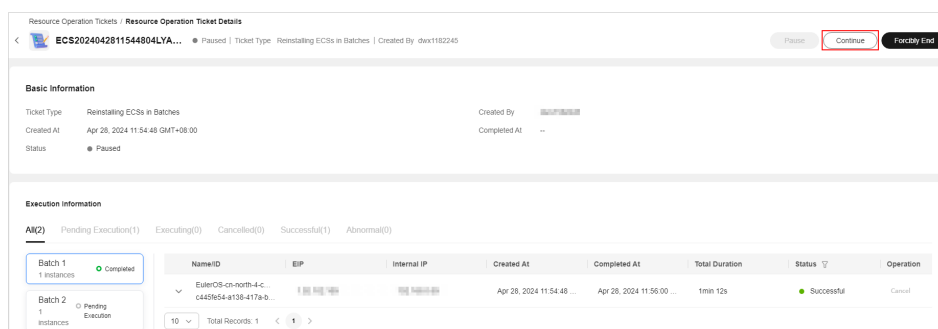
If you select **Automatic** or **Manual** and multiple batches of OS reinstallation tasks are generated, the process will be suspended after each batch of tasks is executed. Perform the following operations to manually continue the next batch of tasks:

- Log in to the [COC](#) console.
- Choose **Task Management > Execution Records**. On the **Resource Operation Tickets** tab, click the target service ticket ID.



- In the service ticket details on the displayed page, click **Continue**.

Figure 1-12 Service ticket details



1.4.6 Changing an OS

Scenarios

If the OS running on the cloud server in a FlexusL instance cannot meet service requirements, you can change the OS to another OS version or type.

Notes

- An OS change does not make any changes to server specifications.
- After the OS is changed, the server IP address remains unchanged.
- Data in all partitions (including the system partition) of the system disk will be cleared, so you are advised to back up the system disk data prior to an OS change.
- An OS change does not affect data in data disks.
- After the OS is changed, the original OS is not retained.
- After you change the OS, you need to deploy services in the new OS.
- After the OS is changed, the server automatically starts.
- Do not perform any operations on the server before the system injects the password, or the login will fail.
- Do not restart or stop the server immediately after the OS is changed. Wait for several minutes to prevent system exceptions.

Constraints

- The OS cannot be changed from an x86 FlexusL instance to an Arm FlexusL instance, such as to a Kunpeng FlexusL instance.
- Windows private images are not supported.
- Application images have the minimum CPU and memory specification requirements. If the specification of a FlexusL instance is low, it cannot be changed to application images. For example, the GitLab application image needs to use at least 2 vCPUs and 8 GiB memory. An instance with 2 vCPUs and 4 GiB memory cannot be switched to the GitLab application image.
- After the OS is changed, the login password is cleared. You need to [reset the password](#), or the login will fail. If you switch to an application image, reset the password [only after the image with the pre-installed application is up and running](#), or the password reset may fail.
- If you use a private image to create a FlexusL instance or change the OS of an existing instance and add HSS to the FlexusL service package, but the server status is **Unprotected**, troubleshoot this issue 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?](#)
- If a private image is created from a server on another cloud platform or downloaded from a third party, the private image may fail to be used to create a FlexusL instance or change the OS of an instance because the password reset plug-in is not installed on the image or the `onekey_resetpasswd` tag is missing. For details, refer to [What Should I Do If a Private Image Cannot Be Used to Create a FlexusL Instance or Change the OS of an Instance Because the Password Reset Plug-in Is Not Installed on the Image or the onekey_resetpasswd Tag Is Missing?](#)

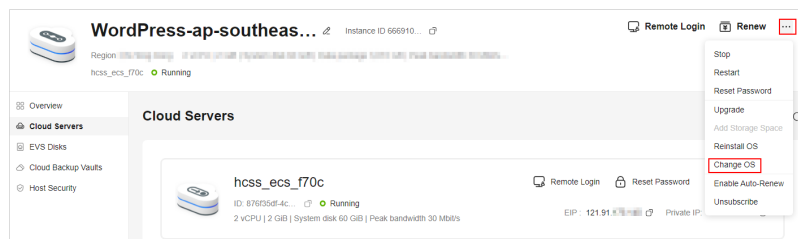
Billing

An OS change does not involve refund or supplementary payment.

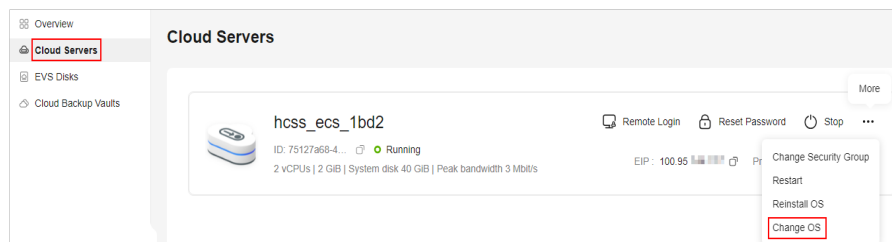
Procedure

1. Log in to the FlexusL console and click a resource card to go to the instance details page.
2. Change the OS using any of the following methods.

- Method 1: Locate the target FlexusL instance, choose **...** > **Change OS**.
- Method 2: On the **Overview** page, choose **...** > **Change OS** in the upper right corner.



- Method 3: On the **Cloud Servers** page, choose **...** > **Change OS** in the row containing the target server.



- Method 4: On the **Cloud Servers** page, click the target server name. In the upper right corner of the displayed page, choose **...** > **Change OS**.
3. Specify the parameters required for changing the OS.
 - Select the image to be switched.

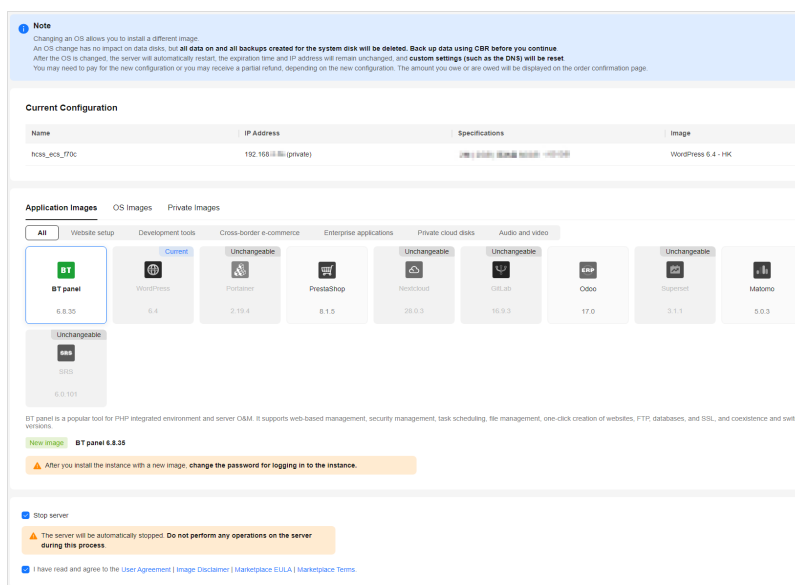
Private images are created from servers on cloud platforms or downloaded from third party platforms. All private images in the same region as your instance under your account are displayed.

You are advised to learn about the constraints and usage of private images by referring to [Managing Private Images](#) before using them.

NOTICE

- The purchased FlexusL instance and the selected private image must be in the same region. For example, if you intend to purchase an instance in the AP-Singapore region, you can only select private images in the AP-Singapore region. To use an image in another region, replicate that image to the current region first. For details, see [Replicating Images Across Regions](#).
- If the message "This image has no password reset plug-in installed or onekey_resetpasswd tagged." is displayed when you use a private image to create a FlexusL instance or change the OS, resolve this issue by referring to [What Should I Do If a Private Image Cannot Be Used to Create a FlexusL Instance or Change the OS of an Instance Because the Password Reset Plug-in Is Not Installed on the Image or the onekey_resetpasswd Tag Is Missing?](#)

- Select **Stop server**. The server must be stopped before its OS can be changed.
- Read and agree to agreement.

4. Click **Submit**.

After the OS is changed, the server automatically starts. When the server status is **Running**, the OS change is complete.

NOTICE

After the OS is changed, the login password is cleared. You need to reset the password, or the login will fail. If you switch to an application image, reset the password **only after the image with the pre-installed application is up and running**.

1.5 Managing Security Groups

1.5.1 Changing a Security Group

This section describes how you can change the security group of a server network interface.

Background

A security group is a collection of access control rules for cloud servers in a VPC. You can define access rules for a security group to protect the cloud servers that are added to this group.

Each network interface comes with a default security group. The default security group rule allows all outgoing data packets and blocks incoming data packets. You can use the default security group or create custom security groups as required.

For more information about security groups, see [security groups](#).

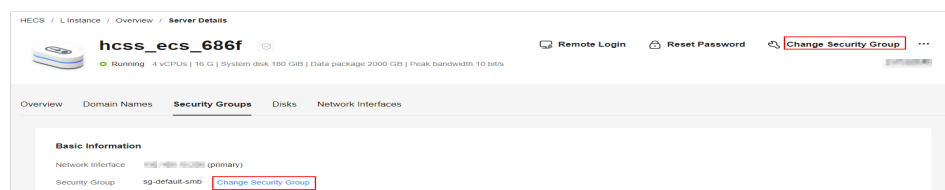
NOTE

If two servers are in the same security group but in different VPCs, the servers cannot communicate with each other. To enable communications between the two servers, connect the two VPCs first. For details, see [Connecting VPCs](#).

Modifying 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** and then click the server name.
3. Click **Change Security Group** in the upper right corner.

Alternatively, click the **Security Groups** tab and click **Change Security Group** in the **Basic Information** area.



4. Select a security group from the list as needed.

You can select multiple security groups. In this case, the access rules of all the selected security groups apply on the cloud server.

To create a security group, click **Create Security Group**. For details, see [Creating a Security Group](#).

NOTE

Using multiple security groups may deteriorate the network performance of the cloud server. You are recommended to select no more than five security groups.

5. Click **OK**.

1.5.2 Configuring Security Group Rules

Scenarios

You can configure security group rules to protect the instances such as cloud servers that are associated with the security group. A security group consists of inbound and outbound rules.

- Inbound rules control incoming traffic to cloud servers in the security group.
- Outbound rules control outgoing traffic from cloud servers in the security group.

Procedure

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** and then click the server name.
3. On the **Security Groups** tab, select **Inbound rules** and click **Add Rule**.
You can click **+** to add more inbound rules.

For details about the configuration examples, see [Security Group Configuration Examples](#).

Figure 1-13 Adding an inbound rule

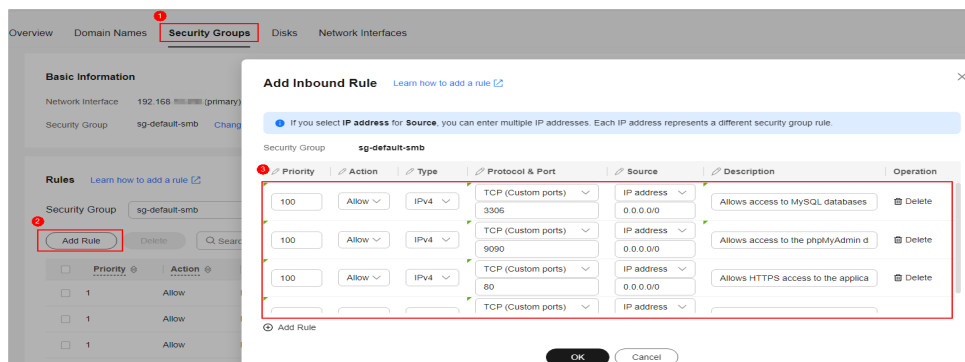


Table 1-7 Inbound rule parameter description

Parameter	Description	Example Value
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default value is 1, indicating the highest priority. The security group rule with a smaller value has a higher priority.	1

Parameter	Description	Example Value
Action	<p>Allow or Deny</p> <ul style="list-style-type: none"> If the Action is set to Allow, access from the source is allowed to cloud servers in the security group over specified ports. If the Action is set to Deny, access from the source is denied to cloud servers in the security group over specified ports. <p>Deny rules take precedence over allow rules of the same priority.</p>	Allow
Type	<p>Source IP address version. You can select:</p> <ul style="list-style-type: none"> IPv4 IPv6 	IPv4
Protocol & Port	<p>The network protocol used to match traffic in a security group rule.</p> <p>Currently, the value can be All, TCP, UDP, ICMP, or more.</p>	TCP
	<p>Destination port used to match traffic in a security group rule. The value can be from 1 to 65535.</p> <p>Inbound rules control incoming traffic over specific ports to instances in the security group.</p> <p>Specify one of the following:</p> <ul style="list-style-type: none"> Individual port: Enter a port, such as 22. Consecutive ports: Enter a port range, such as 22-30. Non-consecutive ports: Enter ports and port ranges, such as 22,23-30. You can enter a maximum of 20 ports and port ranges. Each port range must be unique. All ports: Leave it empty or enter 1-65535. 	22, or 22-30

Parameter	Description	Example Value
Source	<p>The source in an inbound rule is used to match the IP address or address range of an external request. The source can be:</p> <ul style="list-style-type: none">● IP address: If you select IP address for Source, you can enter multiple IP addresses in the same IP address box. Each IP address represents a different security group rule.<ul style="list-style-type: none">- Single IP address: IP address/mask Example IPv4 address: 192.168.10.10/32 Example IPv6 address: 2002:50::44/128- An IP address range in CIDR notation: IP address/mask Example IPv4 address range: 192.168.52.0/24 Example IPv6 address range: 2407:c080:802:469::/64- All IP addresses 0.0.0.0/0 represents all IPv4 addresses. ::/0 represents all IPv6 addresses.● Security group: The source is from another security group. You can select a security group in the same region under the current account from the drop-down list. Instance A is in security group A and instance B is in security group B. If security group A has an inbound rule with Action set to Allow and Source set to security group B, access from instance B is allowed to instance A.● IP address group: The source is an IP address group. An IP address group is a collection of one or more IP addresses. You can select an available IP address group from the drop-down list. An IP address group can help you manage IP address ranges and IP addresses with same security requirements in a more simple way.	IP address: 0.0.0.0/0
Description	<p>Supplementary information about the security group rule. This parameter is optional.</p> <p>The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).</p>	-

4. On the **Security Groups** tab page, select **Outbound rules** and click **Add Rule**. You can click + to add more outbound rules.

Table 1-8 Outbound rule parameter description

Parameter	Description	Example Value
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default value is 1, indicating the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	Allow or Deny <ul style="list-style-type: none">If the Action is set to Allow, access from cloud servers in the security group is allowed to the destination over specified ports.If the Action is set to Deny, access from cloud servers in the security group is denied to the destination over specified ports. Deny rules take precedence over allow rules of the same priority.	Allow
Type	Destination IP address version. You can select: <ul style="list-style-type: none">IPv4IPv6	IPv4
Protocol & Port	The network protocol used to match traffic in a security group rule. Currently, the value can be All , TCP , UDP , ICMP , or more.	TCP
	Destination port used to match traffic in a security group rule. The value can be from 1 to 65535. Outbound rules control outgoing traffic over specific ports from instances in the security group. Specify one of the following: <ul style="list-style-type: none">Individual port: Enter a port, such as 22.Consecutive ports: Enter a port range, such as 22-30.Non-consecutive ports: Enter ports and port ranges, such as 22,23-30. You can enter a maximum of 20 ports and port ranges. Each port range must be unique.All ports: Leave it empty or enter 1-65535.	22, or 22-30

Parameter	Description	Example Value
Destination	<p>The destination in an outbound rule is used to match the IP address or address range of an internal request. The destination can be:</p> <ul style="list-style-type: none">• IP address: If you select IP address for Destination, you can enter multiple IP addresses in the same IP address box. Each IP address represents a different security group rule.<ul style="list-style-type: none">- Single IP address: IP address/mask Example IPv4 address: 192.168.10.10/32 Example IPv6 address: 2002:50::44/128- An IP address range in CIDR notation: IP address/mask Example IPv4 address range: 192.168.52.0/24 Example IPv6 address range: 2407:c080:802:469::/64- All IP addresses 0.0.0.0/0 represents all IPv4 addresses. ::/0 represents all IPv6 addresses.• Security group: The destination is from another security group. You can select a security group in the same region under the current account from the drop-down list. For example, instance A is in security group A and instance B is in security group B. If security group A has an outbound rule with Action set to Allow and Destination set to security group B, access from instance A is allowed to instance B.• IP address group: The destination is an IP address group. An IP address group is a collection of one or more IP addresses. You can select an available IP address group from the drop-down list. An IP address group can help you manage IP address ranges and IP addresses with same security requirements in a more simple way.	IP address: 0.0.0.0/0
Description	<p>Supplementary information about the security group rule. This parameter is optional.</p> <p>The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).</p>	-

5. Click **OK**.

Verifying Security Group Rules

After inbound and outbound rules are added, you can verify whether the rules take effect. Suppose you have deployed a website on a FlexusL instance server. To allow your users to access your website over port 80 (HTTP), you add a security group rule shown in [Table 1-9](#).

Table 1-9 Security group rule

Direction	Protocol/ Application	Port	Source
Inbound	TCP	80	0.0.0.0/0

Linux servers

To verify the security group rule on a Linux server:

1. Log in to the server.
2. Run the following command to check whether TCP port 80 is listened:

```
netstat -an | grep 80
```

If command output shown in [Figure 1-14](#) is displayed, TCP port 80 is listened.

Figure 1-14 Command output for the Linux server

```
tcp      0      0 0.0.0.0:80          0.0.0.0:*        LISTEN
```

3. Enter **http://EIP bound to the server** in the address box of the browser and press **Enter**.

If the requested page can be accessed, the security group rule has taken effect.

Related Operations

On the **Inbound Rules** and **Outbound Rules** tab pages, you can also modify, replicate, or delete existing rules.

Deleting security group rules will disable some functions.

- If you delete a rule with **Protocol & Port** specified as **TCP: 20-21**, you will not be able to upload files to or download them from servers using FTP.
- If you delete a rule with **Protocol & Port** specified as **ICMP: All**, you will not be able to ping the servers.
- If you delete a rule with **Protocol & Port** specified as **TCP: 443**, you will not be able to connect to websites on the servers using HTTPS.
- If you delete a rule with **Protocol & Port** specified as **TCP: 80**, you will not be able to connect to websites on servers using HTTP.
- If you delete a rule with **Protocol & Port** specified as **TCP: 22**, you will not be able to remotely connect to Linux server using SSH.

1.5.3 Configuring Security Groups for Application Images

By default, outbound rules of a security group allow FlexusL instances in it to access external resources. This section describes how you can **configure inbound rules** for multiple application images of FlexusL instances. You can add multiple rules as required.

- For details about more configuration examples, see [Security Group Configuration Examples](#).
- For details about how to configure security group rules, see [Configuring Security Group Rules](#).

WordPress

Table 1-10 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 22	0.0.0.0/0	Allows access to the FlexusL instance using SSH locally.
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	Allows HTTP traffic to the FlexusL instance.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS traffic to the FlexusL instance.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

BT Panel

Table 1-11 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 22	0.0.0.0/0	Allows access to the FlexusL instance using SSH locally.
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.

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

Matomo

Table 1-12 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 22	0.0.0.0/0	Allows access to the FlexusL instance using SSH locally.
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Allows HTTP access to the application dashboard.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS access to the application dashboard.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

Portainer

Table 1-13 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 22	0.0.0.0/0	Allows access to the FlexusL instance using SSH locally.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS access to the application dashboard.
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Allows HTTP access to the application dashboard.
1	Allow	IPv4	TCP: 3306	0.0.0.0/0	Allows access to MySQL databases.

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

GitLab

Table 1-14 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 22	0.0.0.0/0	Allows access to the FlexusL instance using SSH locally.
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Allows HTTP access to the application dashboard.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS access to the application dashboard.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M dashboard.

PrestaShop

Table 1-15 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 22	0.0.0.0/0	Allows access to the FlexusL instance using SSH locally.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS access to the application dashboard.
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Allows HTTP access to the application dashboard.
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.

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M dashboard.

Odoo

Table 1-16 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 22	0.0.0.0/0	Allows access to the FlexusL instance using SSH locally.
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Allows HTTP access to the application dashboard.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS access to the application dashboard.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

Superset

Table 1-17 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 22	0.0.0.0/0	Allows access to the FlexusL instance using SSH locally.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS access to the application dashboard.
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Allows HTTP access to the application dashboard.
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.
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M dashboard.

Nextcloud

Table 1-18 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 22	0.0.0.0/0	Allows access to the FlexusL instance using SSH locally.
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Allows HTTP access to the application dashboard.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS access to the application dashboard.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M dashboard.

SRS

Table 1-19 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 22	0.0.0.0/0	Allows access to the FlexusL instance using SSH locally.
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Allows HTTP traffic to an application.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows HTTPS traffic to an application.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.
1	Allow	IPv4	TCP: 1935	0.0.0.0/0	Allows access to the RTMP livestreaming server.
1	Allow	IPv4	TCP: 1985	0.0.0.0/0	Allows access to the HTTP API server to deliver HTTP-API and WebRTC streams.
1	Allow	IPv4	TCP: 8080	0.0.0.0/0	Allows access to the HTTP livestreaming server to deliver HTTP-FLV and HLS streams.

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 8000	0.0.0.0/0	Allows access to the WebRTC media server.

1.6 Managing Images

1.6.1 Managing Application Images

Scenarios

FlexusL provides various featured application images. An application image contains not only the underlying OS (Ubuntu 22.04), but also application software, initialization data, and runtime environment required by the application. You can use application images to quickly deploy applications out-of-the-box, minimizing the need for separate upload and installation.

You can log in to the visual dashboard of the application image for quick configuration. This section describes the precautions for using application images and how to log in to the image application dashboard.

Precautions

If a FlexusL instance is created using an application image, **ensure that the application has been installed from the image and running properly on the instance** before you reset the instance password, or restart, start, or stop the instance. Otherwise, you may fail to log in to the image application dashboard.

Logging In to the Image Application Dashboard

If it is your first login to the dashboard, you need to **initialize the application preinstalled in the image**. If it is not the first login, you can **access the dashboard** directly.

Step 1: Initializing the Application Pre-installed in the Image

During the initialization, you need to set the information about the application. Different applications require different initialization operation. Perform the corresponding operation based on your application. **Table 2** describes how to initialize the application pre-installed in the image.

Table 1-20 Initializing the application pre-installed in the image

Application Image	Step 1: Obtain or Set the Username and Password for Logging in to the Image Application Dashboard	Step 2: Initialize the Application Pre-installed in the Image
BT panel	Obtain the initial username and password from the password.txt file of the application image. For details, see Obtaining the initial username and password from the password.txt file .	Initializing BT Panel
WordPress	No initial username and password preset in the image. Set the username and password during the initialization and remember them.	Initializing WordPress
Odoo		Initializing Odoo
Matomo		Initializing Matomo
Portainer		Initializing Portainer
GitLab	Obtain the administrator username and password for logging in to the dashboard. For details, see Obtaining the administrator username and password from the application O&M dashboard .	Initializing GitLab
Prestashop		Initializing PrestaShop
Superset		Initializing Superset
Nextcloud		Initializing Nextcloud
SRS	No username and password.	Understanding the SRS Interface

- Obtaining the initial username and password from the password.txt file
[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. The administrator username is **administrator**.

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

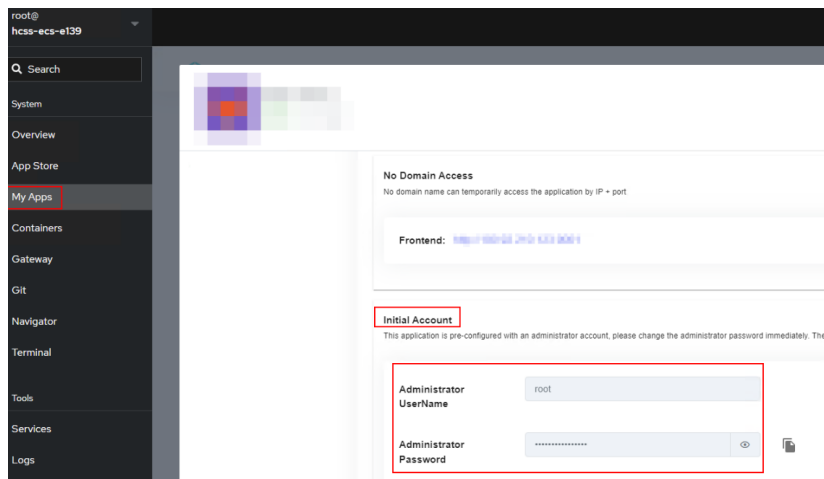
After the application is initialized, change the password on the dashboard for easy management.

NOTE

- If the password is changed, the initial password will be invalid. Remember the new password.
- Obtaining the administrator username and password from the application O&M dashboard
 - a. In the address bar of a local browser, enter **http://EIP:9000** to log in to the application O&M dashboard.

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 **Initial Account** to view the username and password of the administrator.

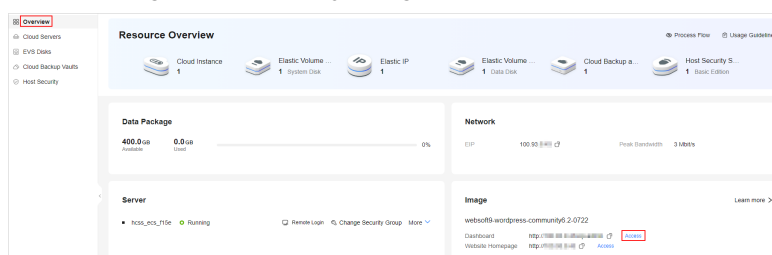


Step 2: Logging in to the Image Application Dashboard

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.

NOTE

For the Prestashop application image, log in to the dashboard using the encrypted address generated when you log in to the dashboard for the first time.



1.6.2 Managing Private Images

Scenarios

You can use a private image to quickly create a FlexusL instance with the same configuration as the image, or use a private image to change the OS.

Private images are created from servers on cloud platforms or downloaded from third party platforms. They can be used by FlexusL only after being created or imported using [Image Management Service \(IMS\)](#).

Constraints

Table 1-21 Restrictions on private images of FlexusL instances

Item	Description
Region	The cloud server and the private image must belong to the same region . Otherwise, the image cannot be used to create the cloud server.
Server architecture	Only x86 is supported.
Image type	<p>Only system disk images are supported. Data disk images and full-servers images are not supported.</p> <ul style="list-style-type: none">Linux system disk images only support the following image sources: free Huawei Cloud public Linux images, images created from FlexusL instances that are created using application images, and images you have imported. Other billed Linux images provided by Huawei Cloud are not supported.Windows system disk images with the Bring Your Own License (BYOL) license are supported. <p>Use SMS to migrate an entire server or migrate an OS unavailable on the cloud to a FlexusL instance.</p>
Specifications	<p>The instance specifications (vCPUs, memory, and system disk capacity) must meet the requirements of the private image. Otherwise, the cloud server may fail to start.</p> <p>For example, Windows images require a minimum of 2 GB memory.</p>
One-click password reset plug-in	<p>If a private image is created from a server on another cloud platform or downloaded from a third party, the private image may fail to be used to create a FlexusL instance or change the OS of an instance because the password reset plug-in is not installed on the image or the onekey_resetpasswd tag is missing. For details, refer to What Should I Do If a Private Image Cannot Be Used to Create a FlexusL Instance or Change the OS of an Instance Because the Password Reset Plug-in Is Not Installed on the Image or the Image's onekey_resetpasswd Tag Is Missing?</p>
Host security	<p>If you use a private image to create a FlexusL instance or change the OS of an instance, and the Host Security Service (HSS) is not protecting the instance, 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?</p>

Preparations

NOTICE

The cloud server and the private image must belong to the same region, or the image is unavailable for selection. For example, if you want to create an instance in the CN-Hong Kong region, you can only select images from the CN-Hong Kong region. To use an image across regions, replicate the image to the target region first. For details, see [Replicating Images Across Regions](#).

Table 1-22 Creating or importing an image using IMS

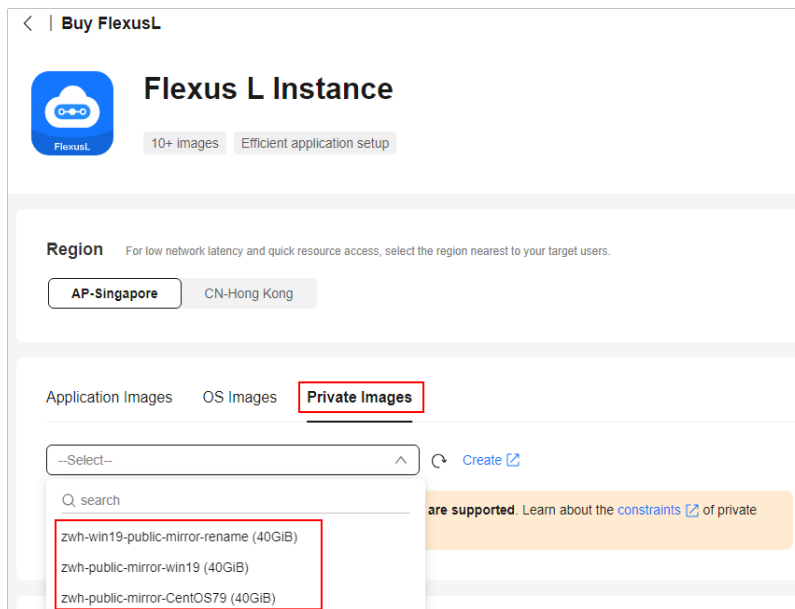
Image Source		Reference
Scenario 1	<p>If your private image is created from a Huawei Cloud ECS or BMS, it can be used in the current region.</p> <p>If you want to use the private image in another region, replicate the image to the region where you want to use it first.</p>	<ul style="list-style-type: none">• Creating a System Disk Image from a Linux ECS• Replicating Images Across Regions
Scenario 2	<p>If your private image is created on another cloud platform or downloaded from a third party, you need to first import the private image using IMS.</p> <p>Refer to the operation guide based on the image file format:</p> <ul style="list-style-type: none">• External image files can be in VMDK, VHD, QCOW2, RAW, VHDX, QED, VDI, QCOW, ZVHD2, or ZVHD format.• ISO files.	<ul style="list-style-type: none">• Creating a Linux System Disk Image from an External Image File• Creating a Linux System Disk Image from an ISO File• Creating a Windows System Disk Image from an External Image File• Creating a Windows System Disk Image from an ISO File
Scenario 3	<p>If you want to use a private image of another account, ask the account owner to share the image with you and replicate the shared image as a private image.</p>	<ul style="list-style-type: none">• Sharing Images• Replicating a Shared Image

Creating a FlexusL Instance Using a Private Image

Create or import a private image using IMS. Select the private image from the image list when creating a FlexusL instance. For details, see [Purchase a FlexusL Instance](#).

NOTE

If your private image is not displayed in the list, check whether the private image is in the same region as the FlexusL instance.

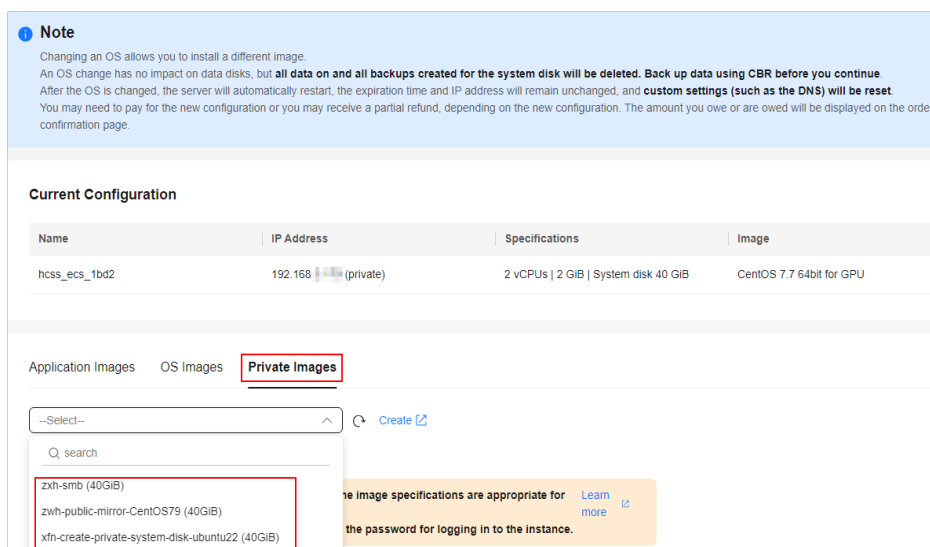


Using a Private Image to Change the OS

Create or import a private image using IMS. Select the private image from the image list when changing the OS of a FlexusL instance. For details, see [Changing an OS](#).

NOTE

If your private image is not displayed in the list, check whether the private image is in the same region as the FlexusL instance.



Related Operations

After you use a private image to create a FlexusL instance or change the OS of an instance, check whether the one-click password reset plug-in has been installed on the instance. If not, install it. With the plug-in, you can reset your instance password.

- If you know the initial password of your private image, install the plug-in by referring to [Installing the One-Click Password Reset Plug-in](#).
- If you forget the initial password of your private image server, install the plug-in by referring to [Setting the Password and Installing the One-Click Password Plug-in](#).

1.7 Managing Disks

1.7.1 Viewing Disk Information and Supported Operations

Background

Elastic Volume Service (EVS) provides scalable block storage that features high reliability, high performance, and a variety of specifications for cloud servers. An EVS disk can be used as a system disk or a data disk.

FlexusL instances contain system disks by default. If your FlexusL instance does not contain any data disk and you need one, you can buy a data disk by referring to [Adding a Data Disk](#).

Constraints

A newly purchased data disk must be initialized in the cloud server OS before you can use it (the system disk does not need to be initialized). For details, see [Initializing a Data Disk](#).

Viewing Disk Information and Supported Operations

1. Log in to the FlexusL console and click a resource card to go to the instance details page.
2. In the list on the left, choose **EVS Disks**. View the disk information and supported operations in the package on the right.
 - Disk information includes the disk name, type, capacity, and specifications.
 - Supported operations include expanding capacity and viewing monitoring data.

1.7.2 Expanding Capacity of a Data Disk

If your disk space is insufficient, you can increase the disk size by expanding capacity.

Constraints

- Expanding the disk capacity does not affect the existing data on the cloud server, but incorrect operations may lead to data loss or exceptions. You are advised to back up the disk data using CBR before expansion.
- Only data disks can be expanded separately. System disks cannot be expanded separately. You can expand the system disk capacity by upgrading the instance specifications. For details, see [Upgrading a FlexusL Instance](#).
- The disk capacity can only be expanded, not reduced.
- The additional capacity has the same expiration time as the FlexusL instance and cannot be unsubscribed from separately.
- The disk can only be expanded when the server is **Running** or **Stopped**.

Billing

The unit price of the additional capacity is the same as the unit price when you add the data disk during the instance purchase.

Prerequisites

The disk has been initialized. If you expand a data disk before it is initialized, you only need to initialize the disk after the expansion and do not need to [extend the disk partition and file system](#). For how to initialize a data disk, see [Initializing a Data Disk](#).

Procedure

1. [Expand the disk capacity on the console](#).
Expanding the disk capacity on the console only enlarges the disk capacity, but not extend the disk partition and file system, so the additional capacity cannot be used directly.
2. [Extend the disk partition and file system](#).
Log in to the server and add the additional capacity to an existing partition or a new partition to make the additional capacity available for use.

Step 1: Expand the Disk Capacity on the Console

1. Log in to the FlexusL console and click a resource card to go to the instance details page.
2. In the list on the left, choose **EVS Disks**. Then click **Expand Capacity**.
3. On the displayed page, enter a new capacity.
If your FlexusL instance contains the cloud backup service, the **Expand Backup Vault** option will be available. Determine whether to expand the backup vault based on your requirements.
 - To expand the backup vault, select **Expand Backup Vault** and enter a new capacity.
 - To retain the vault capacity, ignore this configuration.

Note

Expanding the disk capacity does not affect the existing data on the server, but incorrect operations may lead to data loss or exceptions. You are advised to back up the disk data using CBR before expansion. Data disk capacity and backup vault capacity can only be expanded. Resources added to the package have the same expiration time as the instance, and they cannot be unsubscribed separately. After the payment is successful, you need to **log in to the server and extend the disk partition and file system** to make the additional disk space available. [Learn how: Windows](#) [Linux](#)

Expand Data Disk

Current Capacity

50 GiB

New Capacity

GiB Value range: 51–2048. Data disk capacity cannot be reduced, so enter an appropriate capacity.

Expand Backup Vault The vault capacity must be **at least as big as** the servers you want to back up. If the vault capacity is smaller than the total backup size, **the backup will fail**.

Expiration

2024/07/12 23:59:59 GMT+08:00

Resources added to the package **have the same expiration time as the instance**, and they **cannot be unsubscribed separately**.

4. Click **Buy Now** and complete the payment as prompted.
After the purchase, check whether the disk capacity has increased on the console.

Step 2: Extend the Disk Partition and File System

Log in to the server and extend the partition and file system.

- For Linux, see [Extending Partitions and File Systems for Data Disks \(Linux\)](#).

1.7.3 Adding a Data Disk

Scenarios

Disks of FlexusL instances include system disks and data disks. When a cloud server is created, a system disk is automatically created and attached. You cannot create a system disk separately. A data disk can be added in either of the following ways:

- Purchase the data disk when purchasing a FlexusL instance. The system will automatically attach the data disk to the cloud server.
- Purchase the disk data after a FlexusL instance is purchased. The system will automatically attach the data disk to the cloud server.

This section describes how to add a data disk after a cloud server is created.

Constraints

- An FlexusL instance only supports one data disk. If there is already a data disk, no more data disks can be added.

NOTE

- Data disks can be added only on the FlexusL console. You cannot add and attach data disks to FlexusL instances on the EVS console or attach existing data disks.
- Added data disks have the same expiration time as their FlexusL instances. They cannot be detached or unsubscribed from separately.

- The data disk can only be added when the server is **Running** or **Stopped**.

Billing

The unit price of the added data disk is the same as the price when you add the data disk during the instance purchase.

Procedure

1. Log in to the FlexusL console and click a resource card to go to the instance details page.
2. Click **Add Resource** in the upper right corner.
3. Select the resource you want to add.

Note
An instance package can contain only one resource of the same service type. If a resource has been added to the package, no more resources of such service type can be added. The package can be expanded only when the instance is running or stopped.

Data Disk (EVS)
Provides persistent block storage. With data redundancy and cache acceleration, EVS delivers highly reliable, durable, low-latency, stable storage. **¥5.00** /month ^

Data Disk Capacity: GB General Purpose SSD V2 | Max. IOPS 3,000, Max. throughput: 125 MiB/s

Expiration
2024/07/12 23:59:59 GMT+08:00
Resources added to the package have the same expiration time as the instance and cannot be removed or unsubscribed separately.

Agreement
 I have read and agree to the [User Agreement](#).

NOTE

- The system automatically attaches the added data disk to the cloud server of the FlexusL instance.
 - The added data disk must be initialized in the cloud server OS before you can use it. For details, see [Initializing a Data Disk](#).
 - The added data disk has the same expiration time as the FlexusL instance.
4. Read and agree to the agreement, click **Buy Now**, and complete the purchase. You can see the added data disk on the console.

1.8 Managing Backups

1.8.1 Viewing Backup Information and Supported Operations

Background

Cloud Backup and Recovery (CBR) enables you to back up cloud servers and disks with ease. In case of a virus attack, accidental deletion, or software or hardware fault, you can restore data to any point in the past when the data was backed up.

CBR involves backups, vaults, and policies.





- A backup is a copy of a particular chunk of data and is usually stored elsewhere so that it may be used to restore the original data in the event of a data loss.



- CBR stores backups in vaults. If your server contains the cloud backup service, the cloud servers or disks will be associated with the corresponding vault, and cloud server backups or cloud disk backups generated will be stored in the associated vault.
- There are backup policies and replication policies.
 - Backup policies: To perform automatic backups, configure a backup policy by setting the execution times of backup tasks, the backup cycle, and retention rules, and then apply the policy to a vault.
 - Replication policies: To automatically replicate backups or vaults, configure a replication policy by setting the execution times of replication tasks, the replication cycle, and retention rules, and then apply the policy to a vault. Replicas of backups must be stored in replication vaults.

For more information, see [What Is CBR?](#)

Procedure

1. Log in to the FlexusL console and click a resource card to go to the instance details page.
2. In the list on the left, choose **Cloud Backup Vaults**. View the vault information and supported operations in the package on the right.

Details	Description
Disk Name/ID	Name and ID of the EVS disk, which cannot be changed You can click  to copy the disk ID.
Vault Status	A vault can be in any of the following states:  : The vault is available.  : The vault expires.  : The vault is abnormal.
Backup Type	Backup type of a cloud server is server backup, which backs up all EVS disks (system and data disks) on the server.
Backup Policy Status	Whether the backup policy is enabled. The policy is enabled by default after you create the cloud server. When you enable a backup policy, you can click the policy name to view the policy details.
Associated Server	Server that has been associated with the vault
Used/Total Vault Capacity	Used capacity and total capacity of the vault, in GB. The vault capacity usage is also displayed.

Details	Description
Operation	<ul style="list-style-type: none">Modifying an applied policy: Click  to modify the backup policy. For details, see Modifying a Policy.Viewing monitoring data: Click  to view backup monitoring data.

1.8.2 Associating a FlexusL Instance with a Server Backup Vault

You can associate a FlexusL instance with a server backup vault on the CBR console, rather than the FlexusL console.

NOTE

FlexusL instances only support server backup vaults.

- Associate a FlexusL instance server with a vault.
 - On the CBR console, choose **Cloud Server Backups** from the left navigation pane and click **Buy Server Backup Vault**. On the displayed page, select a FlexusL instance server you want to back up. For details, see [Purchasing a Server Backup Vault](#).
 - Associate a FlexusL instance server with an existing vault. For details, see [Associating a Resource with the Vault](#).
- View the vault details. For details, see [Querying a Vault](#).

1.8.3 Backing Up and Restoring a FlexusL Instance

CBR enhances data integrity and service continuity.

After your FlexusL instance server is associated with a backup vault, you can apply a backup policy to the FlexusL instance for auto backup or back up data manually.

- Method 1: Auto Backup Based on the Backup Policy:** All disks in a FlexusL instance are backed up or restored as a whole.
- Method 2: Manual Backup:** All disks can be backed up or restored as a whole or individually.

If you did not associate a vault with the FlexusL instance server during the purchase, you can buy a vault and associate it with the FlexusL instance server later on the CBR console. For details, see [Associating a FlexusL Instance with a Server Backup Vault](#).

Prerequisites

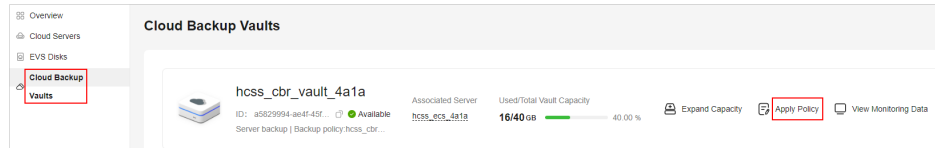
Your FlexusL instance server has been associated with a server backup vault.

Method 1: Auto Backup Based on the Backup Policy

After you associate a cloud backup vault with a FlexusL instance server during the purchase, the cloud server can be automatically backed up based on the policy. You can view or modify the backup policy on the FlexusL console.

Step 1 Log in to the FlexusL console and click a resource card to go to the instance details page.

Step 2 On the displayed page, choose **Cloud Backup Vaults** from the left navigation pane and click **Apply Policy** in the upper right corner.



Step 3 View or set the backup policy parameters.

For details about the parameters, see [Backup policy parameters](#).

NOTE

More frequent backups create more backups or retain backups for a longer time, protecting data to a greater extent but occupying more storage space. Set an appropriate backup frequency as needed.

Edit Policy

Basic Information

Policy Name

Status Enabled Disabled

Backup Rule

Current rule:
Automatically perform weekly backups at 03:00 on the following days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday.
The initial backup is a full backup. All subsequent backups are incremental backups.

Backup Frequency Weekly Day based

Automatically perform backups every Mon Tues Wed Thur Fri Sat Sun

Execution Time Select All Invert Selection

00:00	01:00	02:00	03:00	04:00	05:00	06:00	07:00
08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00
16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00

Timezone

Full Backup Enable
Enabling full backup improves your data reliability, but they will use more storage space.

Retention Rule

Current rule: Permanent

Type Backup quantity Time period Permanent

After the policy's retention rule type is changed from Time period to Permanent, the new retention rule will be applied only to new backups, and backups generated before this change will be kept and deleted based on the old rule. [Learn more](#)

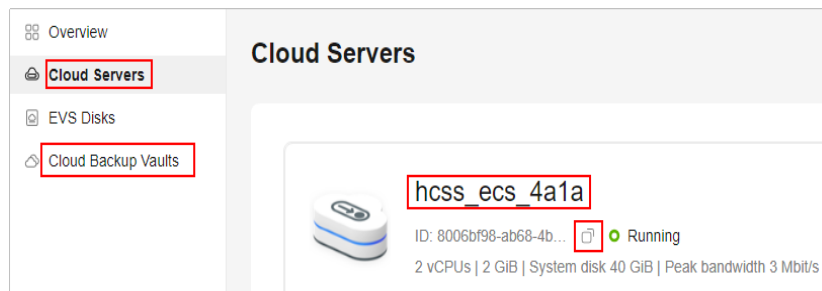
Step 4 Click Create Now.

After the backup policy is created, cloud servers are automatically backed up based on the policy.

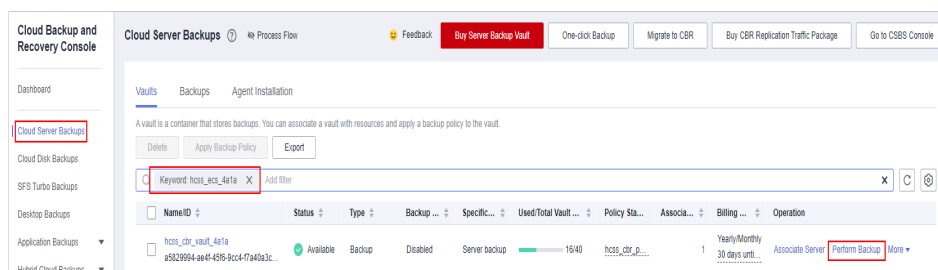
----End

Method 2: Manual Backup

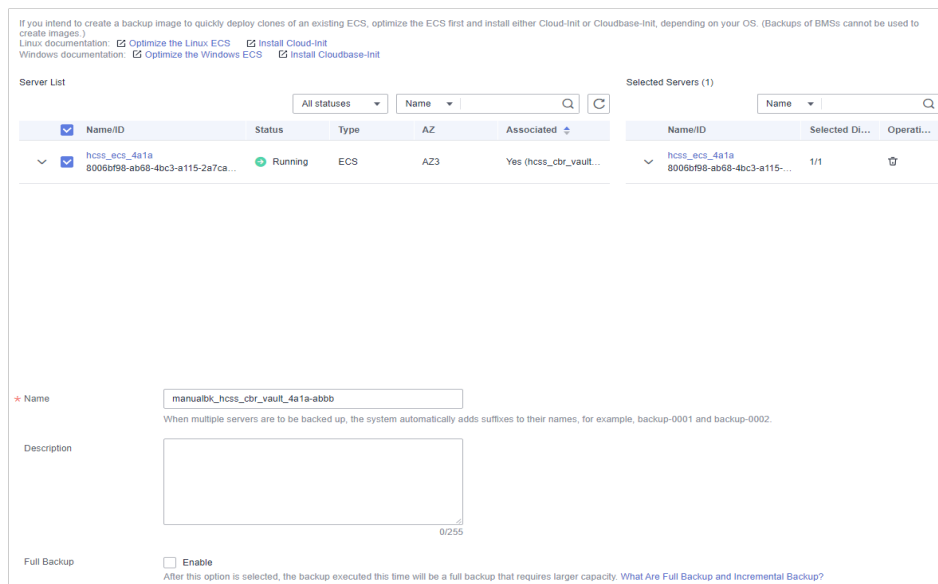
1. On the FlexusL console, obtain the server name or ID, or the backup vault name or ID so that you can quickly find the associated vault on the [CBR console](#).
 - If you associate a vault with a FlexusL instance server during the purchase, search by either server name or ID, or vault name or ID. Log in to the FlexusL [console](#), click a resource card, and choose **Cloud Servers** or **Cloud Backup Vaults** from the left navigation pane on the displayed page to obtain the server name or ID, or vault name or ID.



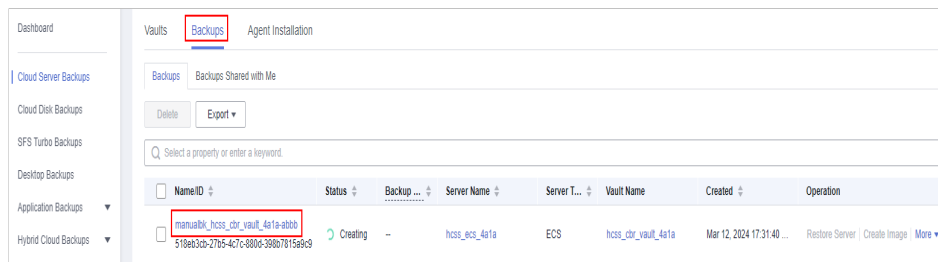
- If you associate a vault with a FlexusL instance server on the CBR console after the FlexusL instance is created, search by server ID.
- 2. Log in to the **CBR console** and choose **Cloud Server Backups**. On the **Vaults** tab in the right pane, search for the vault using the obtained vault name or ID, and click **Perform Backup** in the **Operation** column.



- 3. Set a backup name and determine whether to enable **Full backup**.
Full Backup: If enabled, a full backup task will be performed for the cloud server. If not, an incremental backup task will be performed.



- 4. Click **OK** to start the backup immediately.
You can view the created backup on the **Backups** tab page and use the backup to restore data when needed.



Restoring a Cloud Server

After backing up the cloud server data, you can use the backup to restore the server. For details, see [Restoring from a Cloud Server Backup](#).

1.8.4 Expanding the Vault Capacity

If your vault space is insufficient, you can increase the vault size by expanding capacity.

Constraints

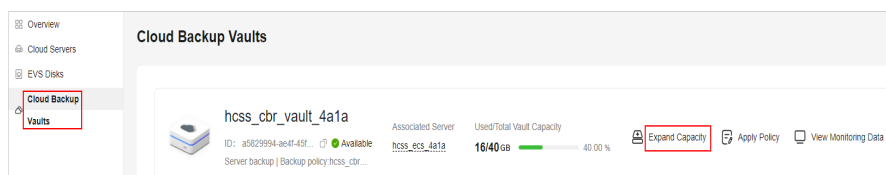
- The vault capacity can only be expanded, not reduced.
- The additional capacity has the same expiration time as the FlexusL instance and cannot be unsubscribed from separately.
- The disk can only be expanded when the server is **Running** or **Stopped**.

Billing

The unit price of the additional capacity is the same as the price when you add the vault during the instance purchase.

Procedure

1. Log in to the FlexusL console and click a resource card to go to the instance details page.
2. Choose **Cloud Backup Vaults** and click **Expand Capacity**.



3. On the displayed page, enter a new capacity.
The vault capacity must be at least as big as the servers you want to back up. If the vault capacity is smaller than the total capacity to be backed up, the backup task will fail. For example, if your system disk and data disks use 80 GB, the vault capacity must be greater than 80 GB. Otherwise, the backup will fail.
4. Click **Buy Now** and complete the payment as prompted.
After the purchase, check whether the vault capacity has increased on the console.

1.9 Managing Domain Names

1.9.1 Overview

To enable a website or web application to be directly accessed using a domain name over the Internet, you need to register a domain name, license the website or web application, and configure DNS. Refer to this topic when you add a domain name and configure DNS for a FlexusL instance.

Process of Accessing a Website Using a Domain Name

1. Register a domain name.
2. Purchase a FlexusL instance.
3. Apply for ICP licensing for the website and domain name.

According to the requirements of the Ministry of Industry and Information Technology (MIIT), to open a website, you must apply for ICP licensing for the website and domain name. You can apply for ICP licensing through Huawei Cloud ICP License Service. Huawei Cloud provides you with free ICP licensing services. For details, see [ICP Filing Process](#).

NOTE

Applying for ICP licensing is only allowed when you will use the FlexusL instances for more than three months (the total duration after multiple renewals).

4. Add a domain name and configure record set for it.

Website services can be provided only after the added domain name is resolved successfully.

Relationships Between Domain Name Registration, Resolution, and Licensing

- You can only configure record sets for a registered domain name.
The registrar and DNS service provider of a domain name can be different. The DNS server settings identify the DNS service provider of the domain name.
 - By default, Huawei Cloud Domain Name Service (DNS) is used to resolve domain names registered with Huawei Cloud. You can set a different DNS service provider by modifying the DNS server settings of the domain name.
 - A domain name registered with Huawei Cloud can be resolved only after record sets are configured for the domain name.
 - If another DNS service provider takes care of domain name resolution, you need to configure record sets for the domain name at the DNS service provider.
- According to MIIT, the web servers and domain name must be filed if you want to host a website in the Chinese mainland. You need to apply for ICP licensing after the domain name is registered and the website is set up.

- ICP licensing is irrelevant to domain name resolution. Accessing a website using a domain name involves the following two phases:
 - The web browser obtains the IP address of the website from the DNS server.
 - The web browser accesses the website using the obtained IP address.

Domain name resolution is implemented at the first phase, and ICP licensing is required at the second phase. If the website is not licensed, the web browser cannot access the website using the obtained IP address.

1.9.2 Adding a Domain Name

When you deploy a website on a FlexusL instance, you need to add a domain name for the instance.

Constraints

A domain name that is not registered can be added. After the domain name is added, it must be registered and licensed. If it is not registered and licensed, the website cannot be accessed. To ensure that a domain name can be used normally, register the domain name and complete ICP licensing before adding the domain name.

If the domain name is not licensed, apply for ICP licensing using Huawei Cloud ICP License Service, which provides free ICP licensing. For details, see [ICP Filing Process](#).

Procedure

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 **Domain Names** tab, click **Add Domain Name**.
4. Configure the parameters and click **OK**.

Parameter	Setting
Domain Name	Enter a domain name that will be added for the instance, for example, wpwebsite.com. NOTE A domain name that is not registered can be added. After the domain name is added, it must be registered and licensed. To ensure that a domain name can be used normally, register the domain name and complete ICP licensing before adding the domain name.
Enterprise Project	Select an enterprise project from the drop-down list. Enterprise projects are associated with public zones. You can manage public zones by enterprise project. NOTE This parameter is displayed only when your account is an enterprise account.

5. On the **Domain Names** tab, view the added domain name.
To enable your website to be accessed using the domain name, you need to [configure DNS for it](#).

Related Operations

After a domain name is added, if you want to change the domain name or do not want to use the domain name any longer, you can click **Remove** in the **Operation** column to unbind the domain name from the instance.

NOTE

Removing a domain name will also delete the record sets you configure for the domain name. As a result, the domain name cannot be used to access the website. If you add the domain name again, you need to configure DNS resolution for it again.

1.9.3 Resolving a Domain Name

After a domain name is added, you need to configure DNS for it. Website services can be provided only after the domain name is resolved normally.

Prerequisites

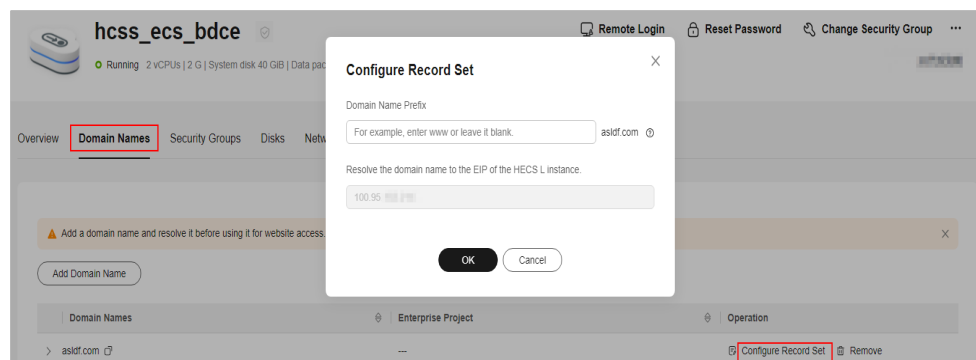
The domain name has been added.

Constraints

- If a domain name has expired or is abnormal, it cannot be resolved. Refer to [What Can I Do If a Record Set Does Not Take Effect?](#)
- If the DNS server settings of the domain name are modified within 24 hours, it takes up to 48 hours for the modification to take effect.

Procedure

1. On the **Domain Names** tab, click **Configure Record Set** in the **Operation** column.
2. Configure the parameters to map the domain name or its subdomain to the EIP of the server, and click **OK**.



Parameter	Setting
Domain Name Prefix	<p>If you enter a prefix, a subdomain is used for website access. Either the domain name or its subdomains can be resolved to the EIP of the instance.</p> <p>Suppose the domain name is wpwebsite.com.</p> <ul style="list-style-type: none">• If the domain name prefix is left empty, wpwebsite.com is resolved to the EIP.• If the domain name prefix is www, the subdomain www.wpwebsite.com is mapped to the EIP.
EIP	The EIP bound to the instance is displayed here automatically.

3. (Optional) Change the DNS server addresses.

If the domain name is not registered with Huawei Cloud or not hosted on Huawei Cloud DNS, the domain name cannot be resolved. To resolve the domain name, contact your DNS provider to change the DNS servers to the following Huawei Cloud DNS servers:

 NOTE

- If the domain name is registered with Huawei Cloud, skip this step.
 - Generally, the changes to DNS servers take effect within 48 hours, but the time may vary depending on the domain name registrar's cache duration.
- ns1.huaweicloud-dns.com: DNS server for regions in the Chinese mainland
 - ns1.huaweicloud-dns.cn: DNS server for regions in the Chinese mainland
 - ns1.huaweicloud-dns.net: DNS server for countries or regions outside the Chinese mainland
 - ns1.huaweicloud-dns.org: DNS server for countries or regions outside the Chinese mainland

4. On the **Domain Names** tab, view the domain name resolution details.

Parameter	Description
Subdomain	The domain name or subdomain that is configured in the record set.
Status	<p>Status of the domain name or subdomain.</p> <ul style="list-style-type: none">• Normal: The domain name is resolved normally and the website can be accessed using the domain name or subdomain.• Disabled: The record set is disabled, and the domain name or subdomain cannot be used to access the website. The record set is still displayed in the list.
Package ID	Package ID of the FlexusL instance.
EIP	The EIP of the instance mapped to the domain name or subdomain.

Parameter	Description
Operation	<ul style="list-style-type: none">• Disable/Enable The domain name registry reviews the legitimacy of the website and restricts website access during domain name licensing. If you have added record sets on the DNS console, you need to disable them and enable them after the licensing is complete.• Delete

In the address box of the web browser, enter **http://Domain name or subdomain** to access the website.

If you want to use HTTPS, [apply for and install an SSL certificate](#) for the instance. After the certificate is installed, you can access the website by entering **https://Domain name or subdomain**.

1.10 Managing Server Security

Background

With intrusion detection, vulnerability management, baseline inspection, and asset management functions, HSS makes it easier to control host security risks.

FlexusL uses HSS basic edition. For details, see [What Is HSS?](#)

Procedure

1. Log in to the FlexusL console and click a resource card to go to the instance details page.
2. In the left navigation pane, choose **Host Security** to view HSS details.

Item	Description
Protection status	HSS is enabled by default and the status is Protected . When the FlexusL instance expires, HSS stops protecting the instance server.
Server status	Status of the server
Detection result	The number of alarms is displayed. HSS supports intrusion detection, vulnerability management, and baseline inspection.
IP address	Private IP or EIP of a server


2 FlexusX

2.1 Purchasing a FlexusX Instance

Scenarios

This section describes how to purchase FlexusX instances on the management console. When purchasing a FlexusX instance, you need to configure the specifications, image, storage, network, and security group for the instance.

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Click **Buy FlexusX**. On the displayed page, configure the parameters below.
3. Select a billing mode.
 - **Yearly/Monthly**: You can select a required duration and pay for the subscription in a single payment.
 - **Pay-per-use**: You do not need to select a required duration. Instead, you will be billed based on how long you use the service.
4. Select a region.

For latency-sensitive services, select a region close to your services to reduce network latency and speed up access. For services that need to communicate with existing cloud services on a private network, select the region where the existing cloud services are deployed.

Exercise caution when selecting a region because it cannot be changed once a FlexusX instance is created.
5. Select instance specifications.

You can select either preset or custom FlexusX instance specifications.
6. Select an image.
 - Public images are standard, widely used images. A public image contains an OS and pre-installed public applications. After your instance is created using a public image, you can deploy applications or software on the instance as required.

- Private images are created on [IMS](#). You can create a private image from a cloud server on Huawei Cloud or another cloud platform, or you can download a third-party image.

Before selecting a private image, you are advised to learn about the usage and constraints of private images described in [Creating a FlexusX Instance from a Private Image or Using a Private Image to Change the OS](#).

NOTICE

The FlexusX instance you are creating and the private image you want to select must belong to the same region. Otherwise, the image cannot be selected for the FlexusX instance. For example, if you want to create a FlexusX instance in the CN-Hong Kong region, you can only select images from the CN-Hong Kong region. If you want to use an image from another region, replicate that image to the current region. For details, see [Replicating Images Across Regions](#).

- A shared image is a private image another user has shared with you.
7. Set storage parameters, including the type and size of the system disk and data disk.
 - If the private image you selected is not encrypted, the system disk will not be encrypted, either. If the image you selected is encrypted, the system disk will be encrypted automatically.
 - You can attach up to 23 data disks to a FlexusX instance.

Click **Show**  to set the following parameters if required:

- **SCSI:** If you select this option, the device type of the data disk is SCSI. For more information about SCSI disks and supported FlexusX instances, see [Device Types and Usage Instructions](#).
 - **Share:** If you select this option, the data disk is sharable. Such a disk can be attached to multiple FlexusX instances.
8. Set network parameters.
 - a. Select an available VPC and subnet from the drop-down list and specify how a private IP address will be assigned.
 - b. Click **Add NIC** to add multiple extension NICs and specify IP addresses for them (including primary NICs).

 NOTE

If you specify an IP address when creating multiple FlexusX instances in a batch:

- This IP address serves as the start IP address.
 - The required IP addresses must be consecutive and available within the subnet.
 - The subnet that contains the specified IP address cannot overlap with other subnets.
- **IPv6 not required/Automatically-assigned IPv6 address:** This parameter is available only for FlexusX instances of specific flavors in a VPC with IPv6 enabled. For details about how to enable IPv6 on a

subnet, see [IPv4 and IPv6 Dual-Stack Network](#). For details about how to check whether a FlexusX instance supports IPv4 and IPv6 dual stack, see "Constraints" in [Dynamically Assigning IPv6 Addresses](#).

By default, the system assigns IPv4 addresses. If you select **Automatically-assigned IPv6 address**, the system assigns IPv6 addresses. In a VPC, a FlexusX instance uses an IPv6 address to access the dual-stack intranet. To access the Internet, you must enable **IPv6 Bandwidth** and select a shared bandwidth. The FlexusX instance then can access the IPv6 Internet through the IPv6 address. After you create a FlexusX instance, you need to enable IPv6 so that the instance dynamically obtains an IPv6 address. For details, see [Dynamically Assigning IPv6 Addresses](#).

NOTE

- IPv6 can only be enabled during instance creation. Once enabled, the configuration cannot be modified. If **IPv6 Bandwidth** is not enabled during instance creation, you can enable it after the instance is created.
 - Dedicated bandwidth is not supported.
- c. Set **Security Group**. You can select an available security group from the drop-down list or create a new one.

This configuration controls access to FlexusX instances within a security group or among security groups, enhancing instance security. You can define access rules for a security group to protect the FlexusX instances that are added to this security group.

When creating a FlexusX instance, you can select multiple security groups (no more than five is recommended). In such a case, the access rules of all the selected security groups apply to the instance.

The security group rules affect the access and use of FlexusX instances. For details about how to configure a security group rule, see [Configuring Security Group Rules](#). Enable the following common protocols and ports as needed:

- Port 80: default port for web page access through HTTP.
 - Port 443: port for web page access through HTTPS.
 - ICMP: used to ping FlexusX instances to check their communication statuses.
 - Port 22: reserved for logging in to Linux FlexusX instances using SSH.
 - Port 3389: reserved for remote desktop login to Windows FlexusX instances.
9. Set EIP parameters.
- An EIP is a static public IP address bound to a FlexusX instance in a VPC. Using the EIP, the instance can communicate with the Internet.
- a. You can select one of the following options as needed:
- **Auto assign**: The system automatically assigns an EIP with a dedicated bandwidth to the FlexusX instance. The bandwidth is configurable.

- **Using existing:** An existing EIP will be assigned to the FlexusX instance. If you select an existing EIP, you cannot create FlexusX instances in batches.
 - **Not required:** A FlexusX instance without an EIP cannot access the Internet. However, it can still be used as a FlexusX instance or be deployed in a cluster on a private network.
- b. Set the EIP type.
- This parameter is mandatory when **Purchase Mode** is set to **Auto assign**.
- **Dynamic BGP:** If changes occur on a network using dynamic BGP, network configurations can be promptly adjusted using the specified routing protocol, ensuring network stability and optimal user experience.
 - **Static BGP** If changes occur on a network using static BGP, network configurations cannot be promptly adjusted and user experience may be affected.
- c. Set **Billed By**.
- This parameter is mandatory when **Purchase Mode** is set to **Auto assign**. If you select **Bandwidth** or **Traffic**, the system will allocate a dedicated bandwidth for you, and the bandwidth is dedicated for one EIP.
- **Bandwidth:** You will be billed based on the amount of bandwidth you configure.
 - **Traffic:** You will be billed based on the actual traffic you have used.
 - **Shared bandwidth:** You will be billed by the bandwidth shared by multiple EIPs.
- d. Set **Bandwidth Size**. Select the bandwidth size (in Mbit/s) based on service requirements.
- e. Set **Release Option**. If you select this option, the EIP will be released when the FlexusX instance is deleted.
10. (Optional) Select **Associated Service**.
- Enable Cloud Eye or HSS if needed.
- If you enable Cloud Eye, an agent will be automatically installed on your FlexusX instance to provide 1-minute fine-grained monitoring of its metrics, such as vCPUs, memory, network, disks, and processes.
 - If you enable HSS, your FlexusX instance will be provided with host security services that scan for weak passwords, system vulnerabilities, brute-force attacks, and unauthorized logins.
- There are three HSS editions: basic edition, enterprise edition, and basic protection trial edition. You can use the basic protection trial edition for free for one month. If you do not pay for it after the free trial expires, host security will become unavailable.
11. Set **FlexusX Instance Name** and **Login Mode**.
- a. You can create a custom FlexusX instance name. If you purchase multiple FlexusX instances at a time, the system automatically sequences these instances.

b. Set **Login Mode**.

- **Password:** A username and its initial password are used for FlexusX instance login authentication.
- **Key pair:** A key pair is used for FlexusX instance login authentication. You can select an existing key pair, or click **Create Key Pair** to create a new one.

 **NOTE**

If you choose to use an existing key pair, ensure that it is available locally, or you will not be able to log in to your FlexusX instance.

- **Password from image:** If a password has been set for the private image, you can select this option to use that password.
- **Set password later:** You can choose to set a password for your FlexusX instance later. If you select this option, remember to set a password after your FlexusX instance is created.

12. Set **Cloud Backup and Recovery**.

Cloud Backup and Recovery (CBR) lets you back up disks and FlexusX instances and use the backups to restore data. After you set **Cloud Backup and Recovery**, the system associates the FlexusX instance with the cloud backup vault and applies the selected backup policy to periodically back up the instance.

For CBR billing details, see [How Is CBR Billed?](#)

You can select one of the following options as needed:

- Create new
 - i. Set the name of the cloud backup vault, which consists of 1 to 64 characters, containing only letters, digits, underscores (_), and hyphens (-). For example, **vault-f61e**. The default naming rule is **vault_XXXX**.
 - ii. Enter the vault capacity, which is required for backing up the ECS. The vault capacity cannot be smaller than that of the ECS to be backed up. Its value ranges from the total capacity of the ECS to 10,485,760 in the unit of GB.
 - iii. Select a backup policy from the drop-down list, or log in to the CBR console and configure a desired one.
- Use existing
 - i. Select an existing cloud backup vault from the drop-down list.
 - ii. Select a backup policy from the drop-down list, or log in to the CBR console and configure a desired one.
- Not required

Skip this configuration if CBR is not required. If you need to enable CBR after creating an ECS, log in to the CBR console, locate the target vault, and bind the ECS to the vault.

13. (Optional) Set **Advanced Options**.

- a. **User Data:** You can inject user data to customize your FlexusX instance. With this configuration, the FlexusX instance automatically injects data the first time it starts up.

- **As text:** allows you to enter the user data in the text box.
- **As file:** allows you to inject script files or other files when you create a FlexusX instance.

For example, if you activate user **root** permission using a script, you can log in to the FlexusX instance as **root**. For details about how to pass user data, see [Passing User Data to ECSs](#).

- b. **Tag:** Adding tags to FlexusX instances helps you better identify and manage your FlexusX instances. You can add up to 10 tags to each instance.

 **NOTE**

Tags added during the instance creation will also be added to the EIP and EVS disks (including the system disk and data disks) of the FlexusX instance. If the instance uses an existing EIP, the tags will not be added to that EIP.

After creating the instance, you can view the tags on the pages providing details about the FlexusX instance, EIP, and EVS disks.

- c. **Agency:** If your FlexusX instance resources need to be shared with other accounts or are delegated to professional personnel or team for management, the tenant administrator creates an agency in IAM and grants permission to manage your FlexusX instance resources.

The delegated account can log in to the cloud system and switch to your account to manage resources. This way, you do not need to share security credentials (such as passwords) with other accounts, ensuring the security of your account.

If you have created an agency in IAM, select the agency from the drop-down list. For more information about agencies, see [Account Delegation](#).

- d. **FlexusX Group:** Select the FlexusX instance group you want to add your FlexusX instance to. A FlexusX instance group applies the anti-affinity policy to the instances in it so that they can be distributed on different hosts. For details about how to create a FlexusX instance group, see [Managing a FlexusX Instance Group](#).

14. Click **Next: Confirm**.

On the displayed page, confirm the configuration details of your FlexusX instance.

- You can select **Set scheduled deletion time** and set the time for deleting the FlexusX instance. This way, the FlexusX instance will be deleted automatically as scheduled.

However, before the scheduled time arrives, you can change it on the instance details page.

NOTICE

Back up data before you set the scheduled deletion time.

- Read and agree to the disclaimer.

Hover your mouse over the price to learn about price details.

15. Click **Submit** and complete the payment.

Follow-Up Operations

- After creating a FlexusX instance, you can remotely connect to the instance to deploy it. For details, see [Logging In to a FlexusX Instance](#). If you did not create a password for your FlexusX instance or if you have forgotten the login password, [reset the password](#) and then log in to the instance.
- If you want to deploy your FlexusX instance by yourself, refer to the instructions in [Setting Up Websites](#).

NOTE

When you set up the environment by referring to [Setting Up Websites](#), ensure that the image version used by the FlexusX instance is the same as that in the tutorial to prevent command execution failures caused by version incompatibility.

2.2 Logging In to a FlexusX Instance

2.2.1 Remotely Logging In to a FlexusX Instance Using VNC


Scenarios

This section describes how to use VNC to remotely log in to a FlexusX instance on the management console.

Prerequisites

- The FlexusX instance for login is in the **Running** state.
- You have obtained the login username and password. If you have forgotten the password, reset it by following [Resetting a Password](#).

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the FlexusX instance you want to log in to, click **Remote Login** in the **Operation** column.
3. Log in to the FlexusX instance following the instructions.
For system security, the password you are entering is hidden by default. After you enter the correct password and press **Enter**, you can successfully log in to the FlexusX instance.
 - For Linux: Enter the username and password following the instructions.
The default username is **root**.

```
Huawei Cloud EulerOS 2.0 (x86_64)
Kernel 5.10.0-60.18.0.50.el8.x86_64 on an x86_64

Hint: Num Lock on

hecsx-3ed6 login: root
Password:
Last login: Tue May 7 14:50:49 on tty1

        Welcome to Huawei Cloud Service

[root@hecsx-3ed6 ~]#
```



2.3 Managing FlexusX Instances

2.3.1 Viewing Details of a FlexusX Instance

Scenarios

After a FlexusX instance is created, you can view and manage it on the FlexusX instance console. This section describes how to view detailed configurations of a FlexusX instance, including the instance name, image, system disk, data disk, security group, and EIP.

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
On the FlexusX instance list page, you can view the FlexusX instances you purchased and their basic information such as private IP addresses.
2. (Optional) In the upper part of the list, enter a FlexusX instance name, IP address, or ID and click  to search for the FlexusX instance.
3. Click the name of the FlexusX instance.
The FlexusX instance details page is displayed.
4. View details of the FlexusX instance.
You can click your desired tab, such as **Summary**, **Disks**, **Network Interfaces**, **Security Groups**, or **Monitoring**, to view the FlexusX instance basic information or monitoring data, add disks or NICs to it, or change its security group.

2.3.2 Resetting a Password

Scenarios

If you did not set a password when purchasing a FlexusX instance, or the password expired or was forgotten, reset the password by following the instructions provided in this section.


Constraints

You can reset the password only when the FlexusX instance is in the **Stopped** or **Running** state. If you reset the password when the FlexusX instance is in **Running** state, the password change will be applied only after the FlexusX instance is restarted.

Prerequisites

- The one-click password reset plug-in must have been installed.
 - If your FlexusX instance was created using a public image, the password reset plug-in was installed on the instance by default.
 - If your FlexusX instance was created using a private image and has no password reset plug-in installed, see [Resetting the Password for Logging In to a Windows ECS Without the Password Reset Plug-in Installed](#) and [Resetting the Password for Logging In to a Linux ECS Without the Password Reset Plug-in Installed](#).
- Do not delete the **CloudResetPwdAgent** or **CloudResetPwdUpdateAgent** process. Otherwise, one-click password reset will not be available.
- DHCP is enabled for the VPC that the FlexusX instance belongs to.
- The FlexusX instance network connectivity is normal.

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the target FlexusX instance, and in the **Operation** column, choose **More > Reset Password**.

You can also select multiple FlexusX instances and click **Reset Password** above the instance list to perform batch operations.

Figure 2-1 Reset Password

Reset Password X

The new password will take effect after the HECS X instance is restarted.

You have selected 1 HECS X instance, 1 of which support password reset. [Show](#)

* New Password

* Confirm Password

* Auto Restart The new password will take effect after the preceding HECS X instances are automatically restarted

Ensure that you save data and then proceed with this operation. Otherwise, HECS X instance data will be lost and cannot be recovered.

Cancel OK

3. Set and confirm a new password as prompted.

If you reset the password for a running FlexusX instance, the password change is applied only after the next restart. Select **Auto Restart**.

NOTE

If the system displays a message indicating that the password cannot be reset, see [Resetting the Password for Logging In to a Windows ECS Without the Password Reset Plug-in Installed](#) and [Resetting the Password for Logging In to a Linux ECS Without the Password Reset Plug-in Installed](#).

The new password must meet the complexity requirements listed in [Table 2-1](#).

Table 2-1 Password complexity requirements

Parameter	Requirement
Password	<ul style="list-style-type: none">• Consists of 8 to 26 characters.• Contains at least three of the following character types:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Digits- Special characters for Windows: \$!@%-_+=+[]:./,?- Special characters for Linux: !@%-_+=+[]:/^,{}?• Cannot contain the username or the username spelled backwards.• Cannot contain more than two consecutive characters in the same sequence as they appear in the username. (This requirement applies only to Windows ECSs.)• Cannot start with a slash (/) for Windows ECSs.


4. Click **OK**.
 - If the FlexusX instance is running when you reset the password, manually restart the instance for the new password to take effect.
 - If the FlexusX instance is stopped, the new password will take effect after you start the instance.

2.3.3 Viewing Failures

Scenarios

You can view the details of failed tasks (if any) in the **Failures** area, including the names and statuses of instances involved in the tasks.

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.

View **Failures** on the right side of buttons for common operations.

2. Click **Failures** to view task details.

The following types of failures can be recorded in the **Failures** area:

- **Creation Failures:** show the failed FlexusX instance creation tasks.
- **Operation Failures:** show the tasks with failed operations and error codes, which help you troubleshoot the faults.

For a failed task, try again. If the failure persists, [submit a service ticket](#) to get technical support.

2.3.4 Reinstalling an OS

Scenarios

If the OS of a FlexusX instance fails to start or requires optimization, reinstall the OS.

Prerequisites

The target FlexusX instance has a system disk attached.


Notes

- After the OS is reinstalled, the IP address of the FlexusX instance remains unchanged.
- Reinstalling the OS clears the data in all partitions, including the system partition, of the system disk. Back up data before reinstalling the OS.
- Reinstalling the OS does not affect data disks.
- Do not perform any operations on the FlexusX instance immediately after its OS is reinstalled. Wait for several minutes until the system successfully injects the password or key. Otherwise, the injection may fail, and the FlexusX instance cannot be logged in to.
- The FlexusX instance will automatically restart after the OS is reinstalled, and only custom settings (such as the DNS) will be reset.

Billing

OS reinstallation is free because the original image will be used.

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the row containing the target FlexusX instance and choose **More > Manage Image > Reinstall OS** in the **Operation** column.
3. Specify the parameters required for reinstalling the OS.
 - Select **Stop FlexusX instance**. The FlexusX instance must be stopped before its OS can be reinstalled.
 - Set **Login Mode**. The credentials are used for logging in to the FlexusX instance.
 - **Password**: A username and its initial password are used for FlexusX instance login authentication.
The initial password of user **root** is used for login authentication in Linux, and the initial password of user **Administrator** is used for login authentication in Windows.
 - **Key pair**: A key pair is used for FlexusX instance login authentication. You can select an existing key pair, or click **Create Key Pair** to create a new one.

NOTE

If you choose to use an existing key pair, ensure that it is locally available. or you will not be able to log in to your FlexusX instance.

- **Password from image:** If a password has been set for the private image, you can select this option to use that password.
- **Set password later:** You can choose to set a password for your FlexusX instance later. If you select this option, remember to set a password after your FlexusX instance is created.

Reinstall OS

Note the following points before you reinstall the OS:
1. An OS reinstallation has no effect on data disks, but all data on and all snapshots created for the system disk will be lost. [Back up the data before you continue.](#)
2. The HECS X instance will be automatically restarted after the OS reinstallation, and custom settings (such as the DNS and hostname) will be reset.
[Hide](#)

Current Configuration

HECS X Instance Name	IP address	Specifications	Image	System ...
hecsx-2914	10.0.0.1 (Private IP) 2420:2023:0000:0000:0000:0000:0000:0000	2 vCPUs 2 GiB	Huawei Cloud EulerOS 2.0 Standard 64 bit(64-bit)	40 GiB

Stop HECS X instance (The HECS X instance must be stopped before its OS can be reinstalled.)

Login Mode: **Password** | Key pair | Inherit Password From Image | Set password later

Password:

You can use the original password or enter a new one.

Confirm Password:

4. Click **OK**.
5. On the **Reinstall OS** page, confirm the OS specifications, read and select the agreement or disclaimer, and click **OK**.

After the OS is reinstalled, the FlexusX instance will automatically restart. When the instance status is **Running**, the OS reinstallation is complete.

Follow-Up Operations

If the OS fails to be reinstalled, install it again. If the second reinstallation attempt still fails, [submit a service ticket](#).

2.3.5 Changing an OS

Scenarios

If the OS running on your FlexusX instance cannot meet service requirements, you can change the OS to another OS version or type.

NOTICE

If you want to use a private image to change the OS of a FlexusX instance, the private image must be in the same region as the instance. Otherwise, the image cannot be selected for the OS change.

Notes

- An OS change does not make any changes to the FlexusX instance specifications.
- After the OS is changed, the IP address of the FlexusX instance remains unchanged.
- After the OS is changed, the original OS will not be retained, and data in all partitions (including the system partition) of the system disk will be cleared, so back up the system disk data before the OS change.
- Changing the OS will not affect data in data disks.
- After the OS is changed, your service running environment must be deployed in the new OS again.
- After the OS is changed, the FlexusX instance will automatically restart.
- Do not perform any operations on the FlexusX instance before the system injects the password or key. Otherwise, the login will fail.


Constraints

- The OS cannot be changed from an x86 FlexusX instance to an Arm FlexusX instance, such as to a Kunpeng FlexusX instance.
- The boot mode (BIOS or UEFI) cannot be changed.

Billing

The new system disk may have a larger capacity after an OS change, so you may be billed more. For details, see [Product Pricing Details](#).

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the row containing the target FlexusX instance and choose **More > Manage Image > Change OS** in the **Operation** column.
3. Specify the parameters required for changing the OS.
 - Select **Stop FlexusX instance**. The FlexusX instance must be stopped before the OS change.
 - Select an image.

If you want to select a private or shared image, create it on the IMS console first.
 - Set **Login Mode**. The credentials are used for logging in to the FlexusX instance.
 - **Password**: A username and its initial password are used for FlexusX instance login authentication.
 - **Key pair**: A key pair is used for FlexusX instance login authentication. You can select an existing key pair, or click **Create Key Pair** to create a new one.

NOTE

If you choose to use an existing key pair, ensure that it is available locally, or you will not be able to log in to your FlexusX instance.

- **Password from image:** If a password has been set for the private image, you can select this option to use that password.
- **Set password later:** You can choose to set a password for your FlexusX instance later. If you select this option, remember to set a password after your FlexusX instance is created.

Change OS

Note the following points before you change the OS:

1. All the data on the system disk, and any snapshots, will be lost. [Back up](#) the data before you continue.
2. The HECS X instance will be automatically restarted after the OS change. Any custom settings (such as the DNS or hostname) will be reset to their default settings.

Current Configuration

HECS X Instance Name	IP address	Specifications	Image	System Disk
hecsx-2914	10.0.0.1 (Private IP)	2 vCPUs 2 GiB	Huawei Cloud EulerOS 2.0 Standard 64 bit...	40 GiB

Stop HECS X instance (The HECS X instance must be stopped before its OS can be changed.)

Image: **Public image** Private image Shared image Marketplace image

--Select OS-- --Select OS version--

Login Mode: **Password** Key pair

Password: Enter a password.

You can use the original password or enter a new one.

Confirm Password: Enter the password again.

Cancel OK

4. Click **OK**.
5. Confirm the OS specifications, read and select the agreement or disclaimer, and click **OK**.

After the OS is changed, the FlexusX instance will automatically restart. When the instance status is **Running**, the OS change is complete.

Follow-Up Operations

If the OS change fails, try again. If the second attempt still fails, [submit a service ticket](#).

2.3.6 Modifying FlexusX Instance Specifications

Scenarios

If the specifications of your FlexusX instance do not meet service requirements, you can modify them.

Notes

- Downgrading FlexusX instance specifications (vCPU or memory) will reduce performance.

- The specifications of a FlexusX instance cannot be modified when the instance is in an intermediate state, such as starting, stopping, resetting the OS, or migrating, or when the capacity of EVS disks used by the instance is being expanded.
- A specification change failure may result in data loss for the FlexusX instance. Back up the data before the change. For details, see [Backing Up a FlexusX Instance](#).

Billing

Modifying specifications will lead to fee changes. For details, see [Pricing of a Changed Specification](#).

Procedure

You can change the specifications of a FlexusX instance to other FlexusX specifications, or you can change a FlexusX instance to an ECS, for even more options.

Changing the Specifications of a FlexusX Instance to Other FlexusX Specifications

Preparations

If there are dependencies between the instance specifications and NICs, after the instance specifications are modified, NIC flapping may occur. Before modifying the specifications, perform the operations below.

NOTE


NIC flapping occurs because NIC retaining is enabled in the image from which the FlexusX Instance is created.

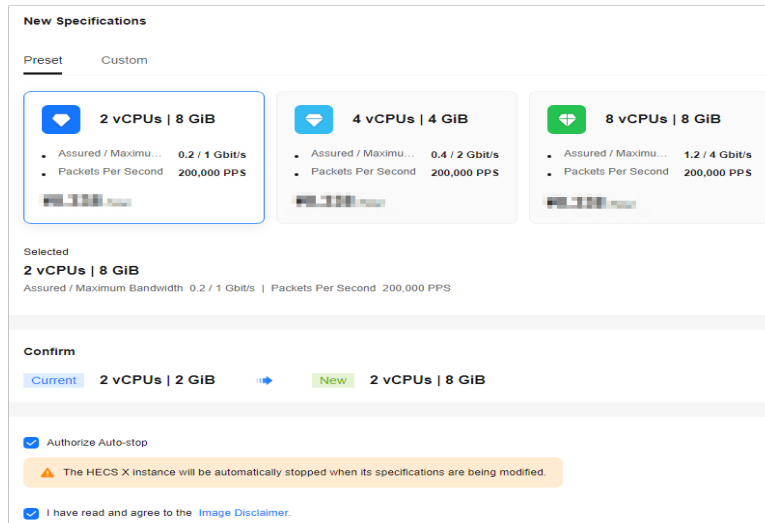
For more information about NIC flapping, see [What Should I Do If NIC Flapping Occurs After My ECS Specifications Are Modified?](#)

- Linux
Run the following commands on the FlexusX instance to delete the files with **persistent** and **net** included in their names from the network rule directory:

```
rm -fr /etc/udev/rules.d/*net*persistent*.rules  
rm -fr /etc/udev/rules.d/*persistent*net*.rules
```

Procedure


1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the row that contains the target FlexusX instance and choose **More > Modify Specifications** in the **Operation** column.
3. On the displayed page, select desired instance specifications.
 - Select the new specifications.
 - Manually stop the FlexusX instance or select **Authorize Auto-stop**.
 - Read and agree to the disclaimer.

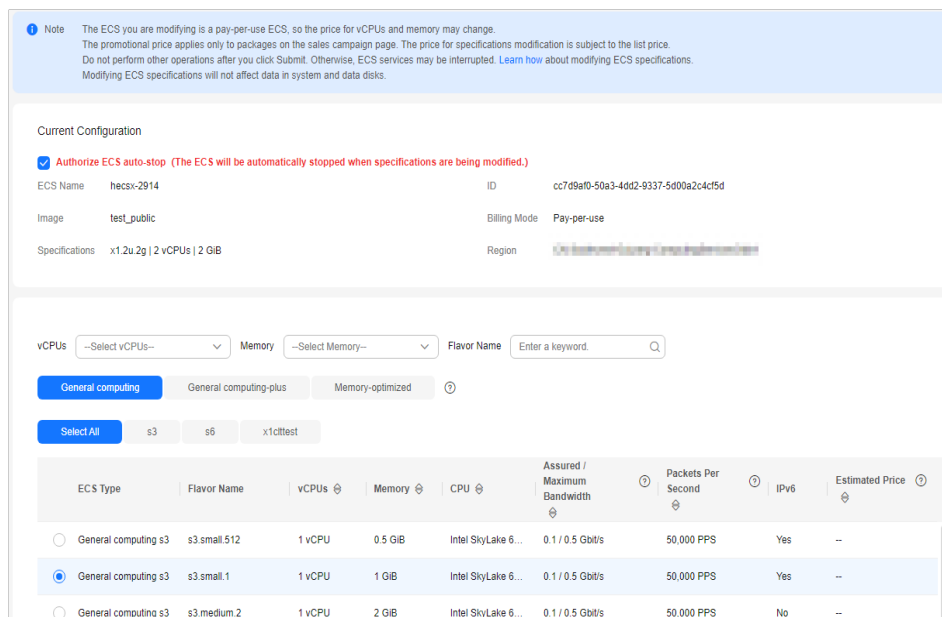


4. Click **Submit**.

Wait until the modification is complete and check whether the specifications have been modified.

Changing a FlexusX Instance to an ECS

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the row that contains the target FlexusX instance and choose **More > Change to ECS** in the **Operation** column.
3. On the displayed page, select desired instance specifications.
 - Before modifying the specifications, manually stop the FlexusX instance or select **Authorize ECS Auto-stop**.
 - Select the new ECS type and specifications.



4. Click **Next**.

5. Confirm the settings, read and select the disclaimer, and then click **Submit**.
Wait until the modification is complete and check whether the specifications have been modified.

Follow-Up Operations

After the specifications of an instance are modified, disks may fail to be mounted. Check disk statuses after the specifications are modified.

- Linux: For details, see [Why Does Disks Fail to Be Mounted After I Modify the Specifications of a Linux ECS?](#)

2.3.7 Managing a FlexusX Instance Group

Scenarios

A FlexusX instance group logically groups FlexusX instances. FlexusX instances in a FlexusX instance group comply with the same policy associated with the group.

Only the anti-affinity policy is supported. This policy enables FlexusX instances in the same FlexusX instance group to run on different hosts for improved reliability, high availability, and disaster recovery.

Constraints

- FlexusX instance groups support only the anti-affinity policy. The failure domain policy is not supported.
- A FlexusX instance group can contain FlexusX instances and ECSs in the same region as it.
- A FlexusX instance can be added to only one FlexusX instance group.
- If the maximum number of FlexusX instance groups is reached, you can contact customer service to increase the quota.

Supported Operations

You can perform the following operations to manage a FlexusX instance group.


Creating a FlexusX Instance Group


Create a FlexusX instance group to apply the same policy to all group members. FlexusX instance groups are independent from each other.

1. Access the page for creating a FlexusX instance group by either of the following ways:

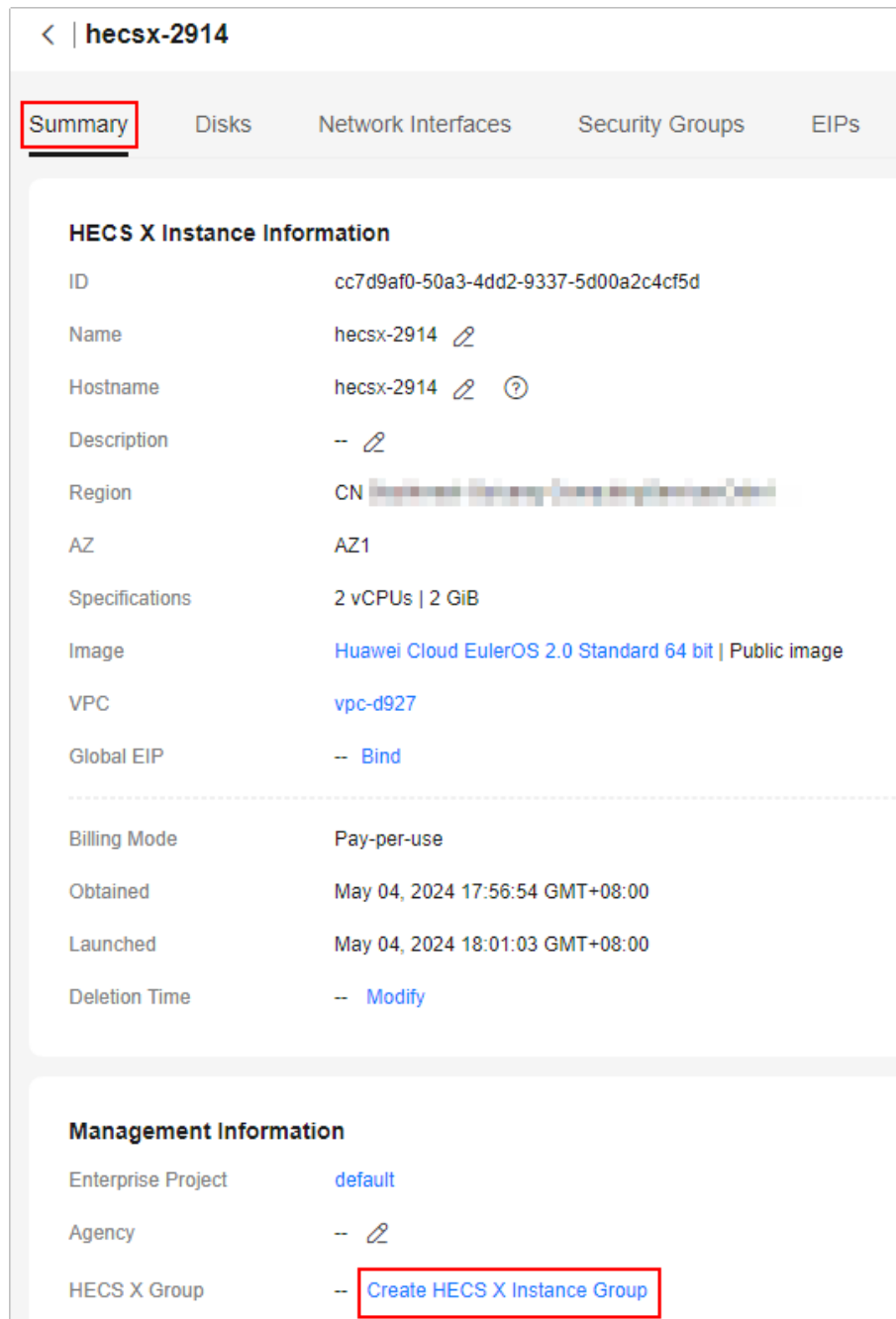
NOTE

Ensure that the FlexusX instance group and the FlexusX instances to be added are in the same region. Otherwise, the FlexusX instances cannot be added.

- Log in to the [ECS console](#), switch to the **ECS Group** page, and click  in the upper left corner to select a region and project.

- Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.






Click the name of a FlexusX instance. On the details page, click **Create FlexusX Instance Group**.



< | **hecsx-2914**


Summary Disks Network Interfaces Security Groups EIPs

HECS X Instance Information

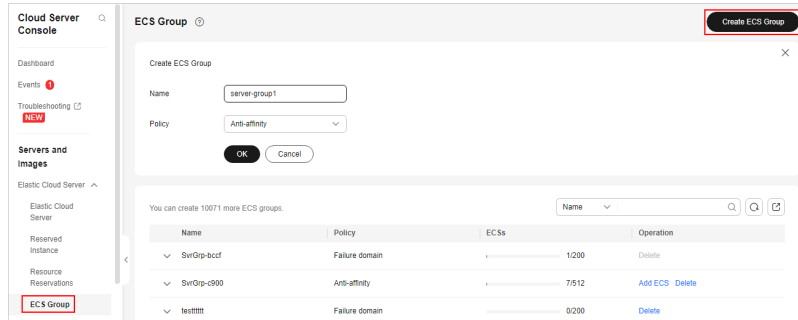
ID	cc7d9af0-50a3-4dd2-9337-5d00a2c4cf5d
Name	hecsx-2914 
Hostname	hecsx-2914  
Description	-- 
Region	CN 
AZ	AZ1
Specifications	2 vCPUs 2 GiB
Image	Huawei Cloud EulerOS 2.0 Standard 64 bit Public image
VPC	vpc-d927
Global EIP	-- Bind

Billing Mode	Pay-per-use
Obtained	May 04, 2024 17:56:54 GMT+08:00
Launched	May 04, 2024 18:01:03 GMT+08:00
Deletion Time	-- Modify

Management Information

Enterprise Project	default
Agency	-- 
HECS X Group	-- Create HECS X Instance Group

2. On the **ECS Group** page, click **Create ECS Group** and set the ECS group name and policy.
Only the anti-affinity policy is supported.



3. Click **OK**.

Adding a FlexusX Instance to a FlexusX Instance Group

To improve service reliability, you can add FlexusX instances to a FlexusX instance group to place these FlexusX instances on different hosts.

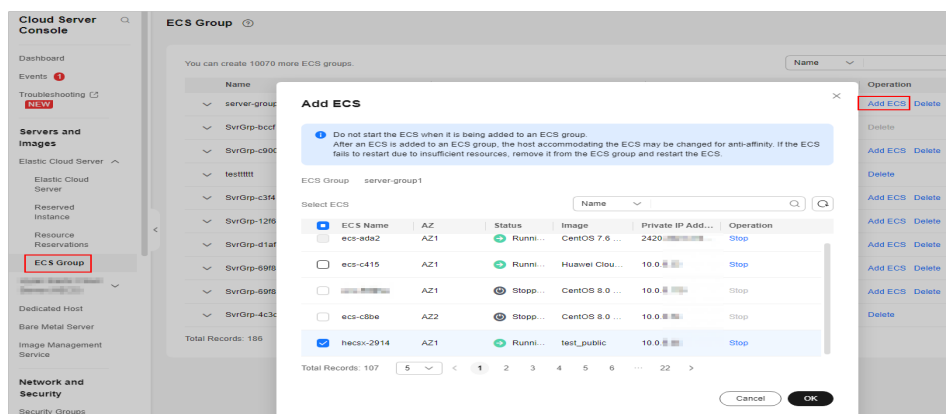
- You can add a FlexusX instance to a FlexusX instance group when you are creating the instance. For details, see [13.d](#).
- You can also add a FlexusX instance to a FlexusX instance group after you create the instance, as described in this part.

NOTE

After a FlexusX instance is added to a FlexusX instance group, the system reallocates a host to run this FlexusX instance to ensure that FlexusX instances in this group are running on different hosts. When the FlexusX instance is being restarted, the startup may fail due to insufficient resources. In such a case, remove the FlexusX instance from its group and try to restart the FlexusX instance again.

- Log in to the [ECS console](#). Switch to the **ECS Group** page, click in the upper left corner, and select a region and project.
- Locate the row that contains the target FlexusX instance group and click **Add ECS** in the **Operation** column.


On the **Add ECS** page, select the FlexusX instance to be added.

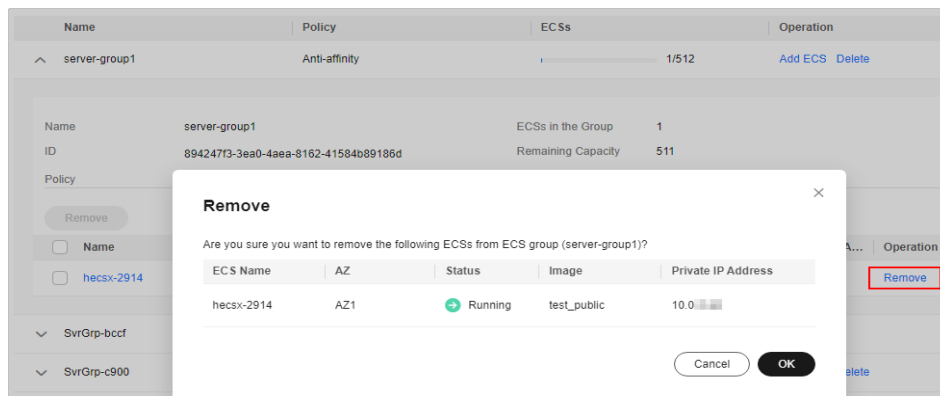


3. Click **OK**.

Removing a FlexusX Instance from a FlexusX Instance Group

After a FlexusX instance is removed from a FlexusX instance group, the FlexusX instance does not comply with the anti-affinity policy anymore.


1. Log in to the [ECS console](#). Switch to the **ECS Group** page, click  in the upper left corner, and select a region and project.
2. Expand the FlexusX instance group information and view the FlexusX instances in it.
3. Locate the FlexusX instance to be removed and click **Remove** in the **Operation** column.



4. Click **OK**.

Deleting a FlexusX Instance Group

Deleting a FlexusX instance group will remove the policy constraints on instances in the group.

1. Log in to the [ECS console](#). Switch to the **ECS Group** page, click  in the upper left corner, and select a region and project.
2. Locate the FlexusX instance group to be deleted and click **Delete** in the **Operation** column.
3. In the displayed dialog box, click **Yes**.

2.4 Managing Images

2.4.1 Overview

Image

An image is a template that contains an OS or service data. It may also contain proprietary software and application software, such as database software.

[Image Management Service \(IMS\)](#) allows you to easily create and manage images. You can create a FlexusX instance using a public image, private image, or shared image. You can also use an existing FlexusX instance or external image file to create a private image.

Private Image

You can use a private image to quickly create FlexusX instances with the same configurations or change the OS of a FlexusX instance.

Operation	Description	Reference
Creating FlexusX instances from a private image	You can use a private image to quickly create FlexusX instances that have the same configurations as the private image.	Creating a FlexusX Instance from a Private Image or Using a Private Image to Change the OS
Using a private image to change the OS	You can use a private image to change the OS of your FlexusX instance.	

You can also create a private image from a FlexusX instance.

Operation	Description	Reference
Creating a private image	<p>You can use a FlexusX instance to create a private image.</p> <p>After the image is created, you can use it to create multiple FlexusX instances with the same configurations or create other cloud servers.</p>	<ul style="list-style-type: none"> • Creating a System Disk Image • Creating a Data Disk Image • Creating a Full-Server Image
Sharing a private image	After creating a private image from a FlexusX instance, you can share the image with other accounts in the same region.	Sharing Images
Replicating a private image	<p>After creating a private image from a FlexusX instance, you can:</p> <ul style="list-style-type: none"> • Use in-region image replication to convert an encrypted image to an unencrypted image, or the other way around. • Replicate the private image to another region and to another account. 	<ul style="list-style-type: none"> • Replicating Images Within a Region • Replicating Images Across Regions
Exporting a private image	After a private image is created from a FlexusX instance, you can export it to a Standard OBS bucket and then download it to your local PC.	Exporting an Image
Deleting a private image	You can delete a private image if you no longer need it.	Deleting Images

2.4.2 Creating a FlexusX Instance from a Private Image or Using a Private Image to Change the OS

Scenarios

You can use a private image to quickly create FlexusX instances with the same configurations or change the OS of a FlexusX instance. For more information, see [Image Management Service](#).

NOTICE

A private image is a regional resource. The FlexusX instances you want to create or change the OS for and the image you want to use must be in the same region. Otherwise, the image cannot be selected.

Billing

Creating a FlexusX instance from a private image or using a private image to change the OS is free of charge.

Constraints

Item	Description
Region	A private image is a regional resource. The FlexusX instances you want to create or change the OS for and the image you want to use must be in the same region. Otherwise, the image cannot be selected.
Cloud server architecture	Only x86 is supported.
Image type	Only Linux images are supported.

Preparations

NOTICE

The FlexusX instance you are creating and the private image you want to select must belong to the same region. Otherwise, the image cannot be selected for the FlexusX instance. For example, if you want to create a FlexusX instance in the CN-Hong Kong region, you can only select images from the CN-Hong Kong region. If you want to use an image from another region, replicate that image to the current region. For details, see [Replicating Images Across Regions](#).

Create a private image before using it. Perform operations based on your scenario.

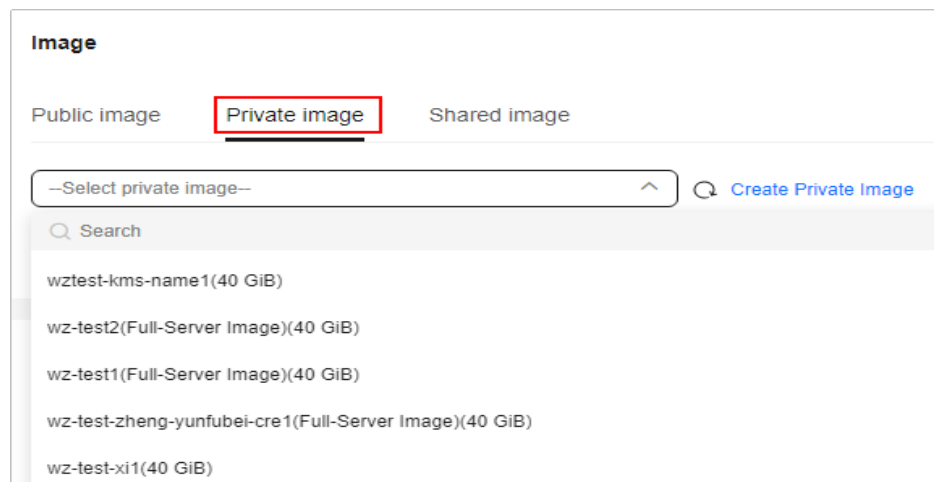
Table 2-2 Creating or importing an image using IMS

Image Source		Reference
Scenario 1	<p>If your private image is created from a Huawei Cloud ECS or BMS, it can be used in the current region.</p> <p>If you want to use the private image in another region, replicate the image to the region where you want to use it first.</p>	<ul style="list-style-type: none"> • Creating a System Disk Image from a Linux ECS • Replicating Images Across Regions
Scenario 2	<p>If your private image is created on another cloud platform or downloaded from a third party, import the private image using IMS.</p> <p>The supported formats for external image files are as follows. The import process depends on the image file format.</p> <ul style="list-style-type: none"> • VMDK, VHD, QCOW2, RAW, VHDX, QED, VDI, QCOW, ZVHD2, and ZVHD • ISO 	<ul style="list-style-type: none"> • Creating a Linux System Disk Image from an External Image File • Creating a Linux System Disk Image from an ISO File
Scenario 3	<p>If you want to use a private image of another account, ask the account owner to share the image with you and replicate the shared image as a private image.</p>	<ul style="list-style-type: none"> • Sharing Images • Replicating a Shared Image

Creating a FlexusX Instance from a Private Image

After creating or importing a private image using IMS, you can select the private image from the image list when creating a FlexusX instance. For details about how to purchase a FlexusX instance, see [Purchasing a FlexusX Instance](#).

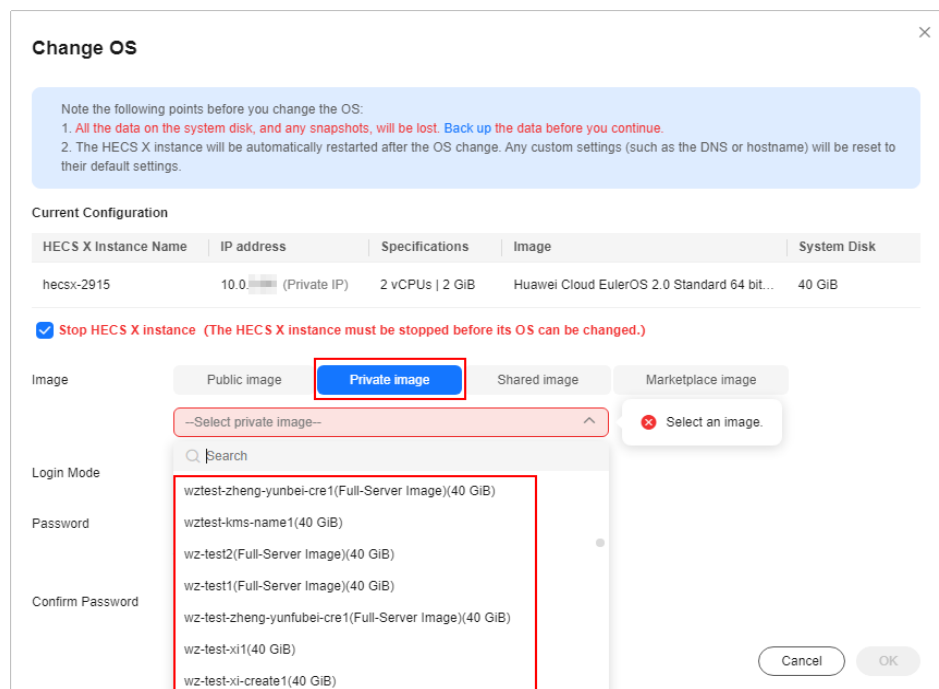
Figure 2-2 Creating a FlexusX instance from a private image



Using a Private Image to Change the OS of a FlexusX Instance

After creating or importing a private image using IMS, you can use the private image to change the OS of your FlexusX instance. For details, see [Changing an OS](#).

Figure 2-3 Using a private image to change the OS of a FlexusX instance



2.4.3 Creating an Image from a FlexusX Instance

Scenarios

You can use an existing FlexusX instance to create a system disk image, data disk image, and full-server image. You can use these images to back up data or quickly create FlexusX instances with the same configurations.

- A system disk image contains an OS and application software for running services. You can use a system disk image to create FlexusX instances and migrate your services to the cloud.
- A data disk image contains only service data. You can export data from a FlexusX instance data disk by creating a data disk image. You can use a data disk image to create EVS disks and use them to migrate your service data to the cloud.
- A full-server image contains all the data of a FlexusX instance, including the data on the data disks attached to the FlexusX instance. A full-server image can be used to rapidly create FlexusX instances with service data.

Constraints

- Only running or stopped FlexusX instances can be used to create private images.

- Do not restart, stop, reset the password of, or reinstall or change the OS of the selected FlexusX instance during image creation.


Billing

- System disk images and data disk images can be used for free.
- If a full-server image is created using Cloud Server Backup Service (CSBS) or Cloud Backup and Recovery (CBR), you will be billed for the storage and cross-region replication traffic on a pay-per-use basis. For details, see [CBR Billing Items](#).
- If a private image is created using a cloud server created from a KooGallery image, the image will be billed based on the KooGallery image pricing details.

Procedure

You can create an image from a FlexusX instance on the IMS console. For details, see [Creating a Private Image](#).

You can also create an image on the FlexusX instance console by following the instructions provided in this section.

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the FlexusX instance and choose **More > Manage Image > Create Image** in the **Operation** column.
3. On the **Create Image** page, configure parameters. Read and agree to the agreement, and click **Next**.

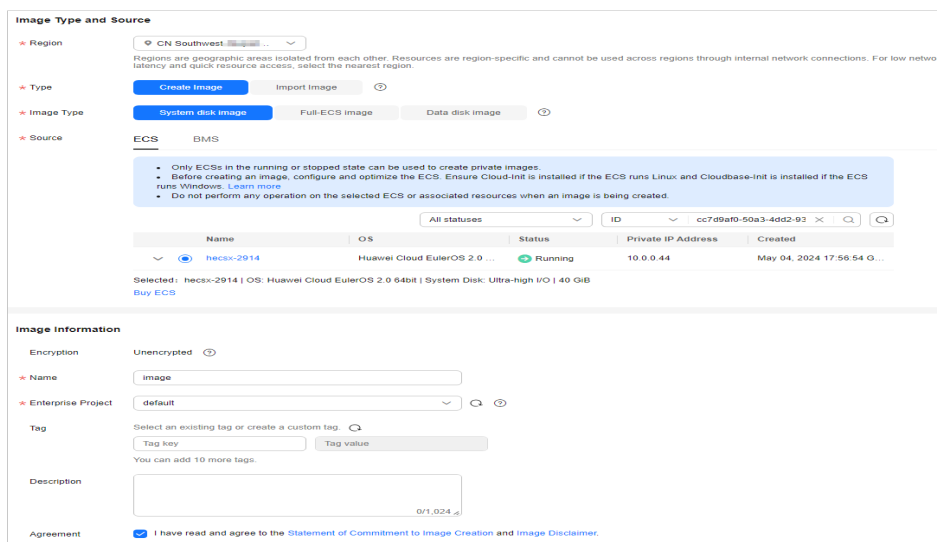


Image Type and Source

Region: CN Southwest

Type: **Create Image** | Import Image

Image Type: **System disk image** | Full-ECS image | Data disk image

Source: **ECS** | BMS

ECS

- Only ECSs in the running or stopped state can be used to create private images.
- Before creating an image, configure and optimize the ECS. Ensure Cloud-Init is installed if the ECS runs Linux and Cloudbase-Init is installed if the ECS runs Windows. [Learn more](#)
- Do not perform any operation on the selected ECS or associated resources when an image is being created.

Name	OS	Status	Private IP Address	Created
hecsx-2914	Huawei Cloud EulerOS 2.0 ...	Running	10.0.0.44	May 04, 2024 17:56:54 G...

Selected: hecsx-2914 | OS: Huawei Cloud EulerOS 2.0 64bit | System Disk: Ultra-high I/O | 40 GiB
Buy ECS

Image Information

Encryption: Unencrypted

Name: image

Enterprise Project: default

Tag: Select an existing tag or create a custom tag. Tag key: Tag value

Description: 0/1,024

Agreement: I have read and agree to the [Statement of Commitment to Image Creation and Image Disclaimer](#).

Table 2-3 Image type and source

Parameter	Description
Region	The region where the FlexusX instance is located is preselected. Retain the default value.
Type	Retain the default value Create Image .

Parameter	Description
Image Type	Select an image type as required.
Source	<ul style="list-style-type: none">• If Image Type is set to System disk image or Full-ECS image, retain the default value.• If Image Type is set to Data disk image, select the data disk of the FlexusX instance from which to create an image.

Table 2-4 Image information

Parameter	Description
Encryption	This parameter specifies whether the image will be encrypted. The value is provided by the system and cannot be changed. <ul style="list-style-type: none">• Only an unencrypted private image can be created from an unencrypted FlexusX instance.• Only an encrypted private image can be created from an encrypted FlexusX instance.
Name	Set a name for the image.
Enterprise Project	Select an enterprise project from the drop-down list. This parameter is available only when you have enabled the enterprise project function, or your account is an enterprise account. To enable this function, contact your customer manager. An enterprise project provides central management of cloud resources on a project.
Tag	(Optional) Set a tag key and a tag value for the image to make identification and management of your images easier.
Description	(Optional) Enter a description of the image.

4. Confirm the settings and click **Submit**.

After the application is submitted, the system automatically returns to the private image list, where you can view the newly created image. The time required for creating an image depends on the EVS disk size, network quality, and the number of concurrent tasks. When the image status changes to **Normal**, the image creation is complete.

 **NOTE**

- Do not perform any operations on the selected FlexusX instance or its associated resources during image creation.
- A FlexusX instance created from an encrypted image is also encrypted. The key used for encrypting the FlexusX instance is the same as that used for encrypting the image.
- An image created from an encrypted FlexusX instance is also encrypted. The key used for encrypting the image is the same as that used for encrypting the FlexusX instance.

Follow-Up Operations

After an image is created, you can use it to:

- Create FlexusX instances.
- Change the OS of existing FlexusX instances.

2.5 Managing EVS Disks

2.5.1 Overview

What Is EVS?

Elastic Volume Service (EVS) offers scalable block storage for FlexusX instances. With high reliability, high performance, and rich specifications, EVS disks can be used for distributed file systems, development and testing environments, data warehouses, and high-performance computing (HPC) scenarios to meet diverse service requirements.

Related Operations

Operation	Description
Adding an EVS Disk	<ul style="list-style-type: none"> • You can purchase data disks when purchasing FlexusX instances. The data disks must be initialized before you can use them. • You can also purchase data disks after purchasing FlexusX instances. <ul style="list-style-type: none"> – Disks created from data sources, such as backups or snapshots, do not need to be initialized. – Disks that are not created from data sources must be initialized before you can use them.
Attaching an EVS Disk	After a FlexusX instance is created, if the EVS disks on the instance cannot meet service requirements, you can attach existing disks to the FlexusX instance.

Operation	Description
Detaching an EVS Disk	<ul style="list-style-type: none">• If the file system on your system disk is damaged and your FlexusX instance cannot be started, you can detach the system disk and attach it to another FlexusX instance as a data disk. After the file system is fixed, you can attach the disk back to the original FlexusX instance as the system disk.• If you want to move a data disk from one FlexusX instance to another in the same region and AZ, you can detach the data disk and then attach it to that FlexusX instance.• If you no longer need an EVS disk, you can detach and delete it.
Expanding the EVS Disk Capacity	If the disk capacity of your FlexusX instance is not enough, you can expand the capacity.
Initializing a Data Disk	Data disks must be initialized before they can be used, regardless of whether they are created together with FlexusX instances or created separately and attached to the FlexusX instances. An initialized data disk does not need to be initialized again. NOTE <ul style="list-style-type: none">• System disks do not need to be initialized.• Data disks containing data do not need to be initialized.

2.5.2 Adding an EVS Disk to a FlexusX Instance


Scenarios

Disks attached to a FlexusX instance are classified into system disks and data disks. A system disk is automatically created and attached when a FlexusX instance is created. You do not need to purchase the system disk separately.

Data disks can be purchased during or after the FlexusX instance creation. If you add a data disk when purchasing a FlexusX instance, the system automatically attaches the data disk to the FlexusX instance. If you buy a data disk after the FlexusX instance is purchased, you need to manually attach the data disk.

This section describes how to add a data disk after a FlexusX instance is created.

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the FlexusX instance, and choose **More > Manage Disk/Backup > Add Disk** in the **Operation** column.
3. Configure parameters for the new EVS disk as prompted.
For instructions about how to set EVS disk parameters, see [Purchasing an EVS Disk](#).

4. Click **Next** to confirm the order and click **Submit** to complete the payment.

Follow-Up Operations

After you add an EVS disk to a FlexusX instance, you must log in to the instance and initialize the disk before you can use it. For details, see [Initializing an EVS Data Disk](#).

NOTE

Disks created from data sources, such as backups or snapshots, do not need to be initialized.

2.5.3 Attaching EVS Disks to a FlexusX Instance

Scenarios

If the disks of a FlexusX instance cannot meet service requirements, for example, due to insufficient disk space, you can attach more available disks to the FlexusX instance.

Constraints


- EVS disks can only be attached to FlexusX instance in the same region as the disks.
- Non-shared disks can be attached only when they are in the **Available** state. Shared disks can be attached when they are in the **In-use** or **Available** state.
- A FlexusX instance must be in the **Running** or **Stopped** state before EVS disks can be attached to it.
- A frozen EVS disk cannot be attached to a FlexusX instance.
- A SCSI EVS disk cannot be attached as the system disk to a FlexusX instance.
- A detached system disk can be used as a data disk for any FlexusX instances, but can only be used as a system disk for the FlexusX instance where it was attached before.
- A detached data disk that is purchased together with a FlexusX instance can only be used as a data disk for this instance.

For more details about attaching disks, see [Attaching a Non-Shared EVS Disk](#) and [Attaching a Shared EVS Disk](#).

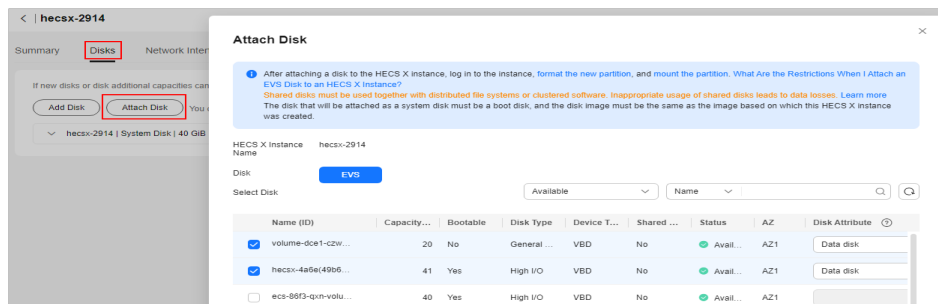
Prerequisites

- EVS disks are available.
For instructions about how to purchase an EVS disk, see [Purchasing an EVS Disk](#).

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Click the name of the target FlexusX instance to which you want to attach a disk.

- The details page of this instance is displayed.
3. Click the **Disks** tab. Then, click **Attach Disk**.
 4. Select the target disk and set disk function as prompted.

Figure 2-4 Attaching an EVS disk

5. Click **OK**.
After the disk is attached, you can view the disk information on the **Disks** tab.

Follow-Up Operations

If the attached disk is newly created, you must log in to the FlexusX instance and initialize the EVS disks before you can use them. For details, see [Initializing an EVS Data Disk](#).

2.5.4 Detaching an EVS Disk from a FlexusX Instance

Scenarios

- If the file system on your system disk is damaged and your FlexusX instance cannot be started, you can detach the system disk and attach it to another FlexusX instance as a data disk. After the file system is fixed, you can re-attach the disk to the original FlexusX instance as the system disk.
- If you want to move a data disk from one FlexusX instance to another in the same region and AZ, you can detach the data disk and then attach it to that FlexusX instance.
- If you no longer need an EVS disk, you can detach and delete it.

Billing

A detached EVS disk will not be automatically deleted, and it will still be billed. To avoid unintended charges, you can delete or unsubscribe from the disk if it is no longer needed.


Constraints

- A system disk can only be detached offline. It means that you can detach the system disk only when its FlexusX instance is in the **Stopped** state.
- After the system disk is detached from a FlexusX instance, the following operations cannot be performed: starting the instance, remote login, resetting the password, changing instance specifications, changing the OS, reinstalling the OS, creating images, creating backups, adding disks, and changing the security group.

Prerequisites

- Before detaching an EVS disk from a running Linux FlexusX instance, you must log in to the instance and run the **umount** command to cancel the association between the disk and the file system. In addition, ensure that no program is reading data from or writing data to the disk. Otherwise, the disk will fail to detach.

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Click the name of the target FlexusX instance from which you want to detach a disk.
The details page of this instance is displayed.
3. Click the **Disks** tab. Locate the target disk and click **Detach**.

2.5.5 Expanding the Capacity of an EVS Disk

Scenarios


If the disk capacity of your FlexusX instance is not enough, you can expand the disk capacity. Expanding the disk capacity do not affect the data in the disk.

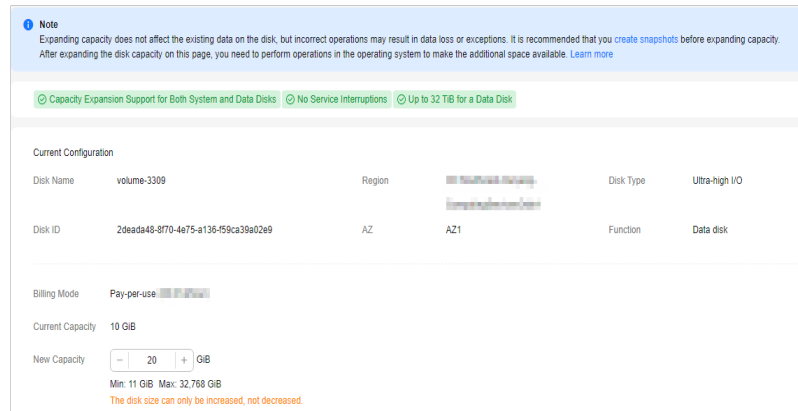
Billing

You will be billed for the additional capacity of a disk after you expand the disk capacity. The billing mode of the additional capacity is the same as that of the disk.

For details, see [Billing for Disks](#).

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the FlexusX instance, and choose **More > Manage Disk/Backup > Expand Disk** in the **Operation** column.
3. Select the disk you want to expand and click **OK**.
4. Set the new capacity of the disk, click **Next**, and complete the expansion as prompted.



Follow-Up Operations

After the disk capacity is expanded, you must log in to the FlexusX instance and extend the partition and file system to the added capacity. If the data disk you expanded has not been initialized, you just need to initialize the data disk after the capacity expansion.

- For Linux, see [Extending Partitions and File Systems for Data Disks \(Linux\)](#).

2.6 Managing Backups

2.6.1 Overview

What Is CBR?

Cloud Backup and Recovery (CBR) enables you to back up cloud servers and disks with ease. In case of a virus attack, accidental deletion, or software or hardware fault, you can restore data to any point in the past when the data was backed up.

CBR protects your services by ensuring the security and consistency of your data.

FlexusX instances can be backed up using cloud server backup and cloud disk backup.

- Cloud server backup (recommended): Use this backup method if you want to back up the data of all EVS disks (system and data disks) attached to a FlexusX instance. All disks on the instance are backed up at the same time, ensuring data consistency.
- Cloud disk backup: Use this backup method if you want to back up the data of one or more EVS disks (system or data disk) attached to a FlexusX instance. This minimizes backup costs on the top of data security.

For more information, see [CBR Architecture](#), [Backup Mechanism](#), and [Backup Options](#).

For the differences between backup, snapshot, and image, see [What Are the Differences Between Backup, Snapshot, and Image?](#)

Related Operations

Operation	Description
Associating a FlexusX Instance with a Backup Vault	If you want to back up a FlexusX instance, associate the instance with a backup vault first.
Backing Up a FlexusX Instance	CBR enhances data integrity and service continuity. After a FlexusX instance is backed up, you can restore its data using the backup.
Expanding Vault Capacity	If the capacity of an existing backup vault is insufficient, the backup may fail. To ensure a successful backup, you can log in to the CBR console to expand the vault capacity. For details, see Expanding Vault Capacity .

2.6.2 Associating a FlexusX Instance with a Backup Vault

Scenarios

You can associate a FlexusX instance with a backup vault during or after the instance is created. The vault can be a new or an existing vault.

This section describes how to associate a FlexusX instance with a new vault after the instance is created.


Constraints

A FlexusX instance can only be associated with a backup vault in the same region as the instance.

Billing

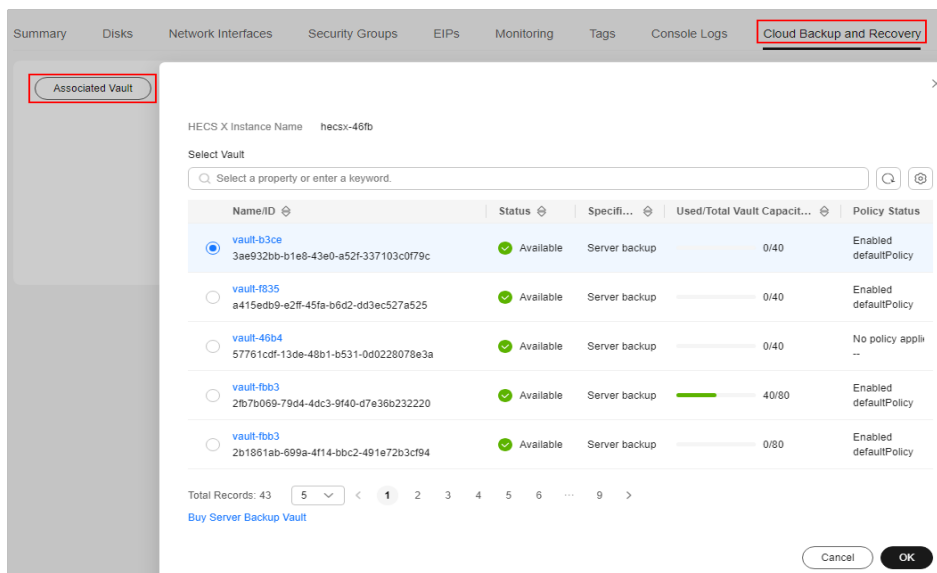
See [CBR Billing Overview](#).

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the FlexusX instance, and choose **More > Manage Disk/Backup** in the **Operation** column.

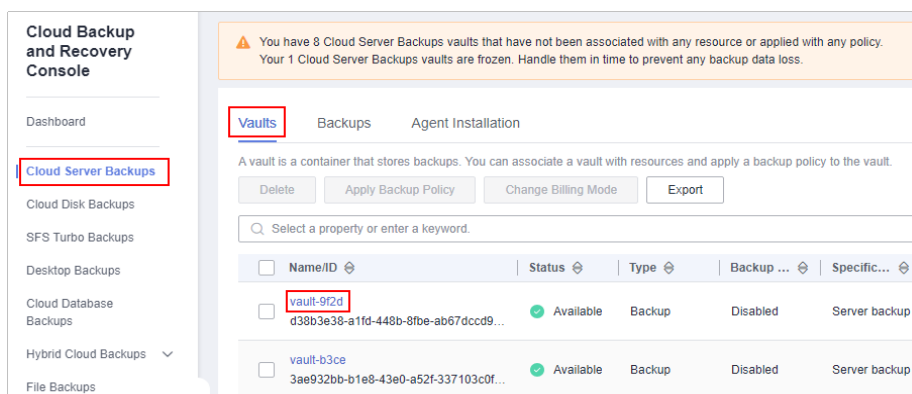
- You can click **Create Server Backup** to purchase a server backup vault on the CBR console. For details, see [Purchasing a Server Backup Vault](#).
- You can click **Create Disk Backup** to purchase a disk backup vault on the CBR console. For details, see [Purchasing a Disk Backup Vault](#).

You can also click the name of the FlexusX instance and associate the instance with an existing vault on the **Cloud Backup and Recovery** tab.



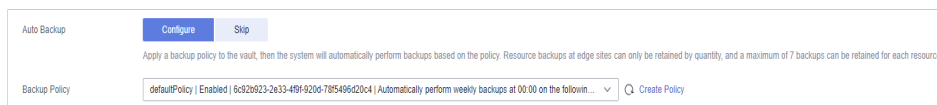
3. View the backup vaults.

After a backup vault is created, click the vault name on the **Cloud Server Backups** or **Cloud Disk Backups** page of the **CBR console** to view the vault information.



Follow-Up Operations

- When you are creating a backup vault, you can configured **Auto Backup** to let the system automatically perform backups based on the policy. You can also manually apply a backup policy to the backup vault. For details, see [Applying a Policy to a Vault](#).



- After a backup vault is created, you can also manually back up a FlexusX instance. For details, see [Backing Up a FlexusX Instance](#).

2.6.3 Backing Up a FlexusX Instance

Scenarios

CBR enhances data integrity and service continuity. You can back up FlexusX instances manually or configure a policy to back them up automatically. This section describes how to manually back up a FlexusX instance.

For more information, see [CBR Architecture](#), [Backup Mechanism](#), and [Backup Options](#).


Prerequisites

The FlexusX instance has been associated with a backup vault. For details, see [Associating a FlexusX Instance with a Backup Vault](#).

Constraints


To ensure the integrity of backup data, do not delete disk data or restart or stop the FlexusX instance during the backup.

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the FlexusX instance, choose **More > Manage Disk/Backup** and click **Create Server Backup** or **Create Disk Backup** in the **Operation** column.

NOTE

If the page for purchasing a backup vault is displayed after you click **Create Server Backup** or **Create Disk Backup**, the FlexusX instance has not been associated with a vault. In this case, [associate the FlexusX instance with a vault](#) first. Then, create a backup by referring to the following part.

- To create a cloud server backup, configure the following parameters:
 - In the server list, the FlexusX instance to be backed up is selected by default. You can click  to view the disks attached to the FlexusX instance and select the disks to be backed up.
 - **Name:** Customize your backup name.
 - **Description:** Enter the supplementary information about the backup.
 - **Full Backup:** If this option is selected, the system will perform full backup for the selected FlexusX instance. The storage capacity used by the backup increases accordingly.
- To create a cloud disk backup:

Click **Perform Backup** in the **Operation** column of the associated backup vault, and then configure the following parameters:

 - In the disk list, all disks are selected by default. You can select the disks to be backed up.

- **Name:** Customize your backup name.
 - **Description:** Enter the supplementary information about the backup.
 - **Full Backup:** If this option is selected, the system will perform full backup for the disks selected. The storage capacity used by the backup increases accordingly.
3. Click **OK**. The system creates a backup immediately.
 4. Click **Go to Backup List**.

On the **Backups** tab page, if the status of the backup is **Available**, the backup task is successful. You can use the backup to restore data when needed.

Follow-Up Operations

- After the cloud server backup is complete, you can use the backup to restore server data or create images on the CBR console. For details, see [Restoring Data Using a Cloud Server Backup](#) and [Using a Backup to Create an Image](#).
- After the cloud disk backup is complete, you can use the backup to restore disk data on the CBR console. For details, see [Restoring from a Cloud Disk Backup](#).

2.7 Managing VPCs

2.7.1 What Is Virtual Private Cloud?

Overview

Virtual Private Cloud (VPC) allows you to provision logically isolated virtual networks for your FlexusX instances. You can define security groups and CIDR blocks for each VPC. This facilitates internal network configuration, management, and change. You can also define rules to control communications between FlexusX instances in the same security group or across different security groups.

For more information about VPC, see [Virtual Private Cloud User Guide](#).

Elastic Network Interface

An elastic network interface is a virtual network card that can be attached to a FlexusX instance in a VPC. You can use network interfaces to manage networks for FlexusX instances. There are two types of elastic network interfaces: primary network interfaces and extension network interfaces.

- A primary network interface is created together with an instance by default, and cannot be detached from the instance.
- An extended network interface is created on the **Network Interfaces** console, and can be attached to or detached from an instance.

Related Operations

Operation	Description
Attaching extension network interfaces	If your FlexusX instance requires multiple network interfaces, you can attach extension network interfaces to it.
Detaching extension network interfaces	You can detach extension network interfaces from your FlexusX instance if they are no longer needed. Only extension network interfaces can be detached from the FlexusX instance. You cannot detach the primary network interface from it.
Changing a VPC	You can move your FlexusX instance from the current VPC to another.
Modifying a private IP address	You can change the private IP address of the primary network interface for a FlexusX instance on the console.
Assigning a virtual private IP address	A virtual IP address serves as a secondary IP address for a network interface. A virtual IP address can be bound to multiple cloud servers to improve server availability.

2.7.2 Attaching Extension Network Interfaces

Scenarios

If your FlexusX instance requires multiple network interfaces, you can attach extension network interfaces to it.

For details, see [Elastic Network Interface Overview](#).

Procedure


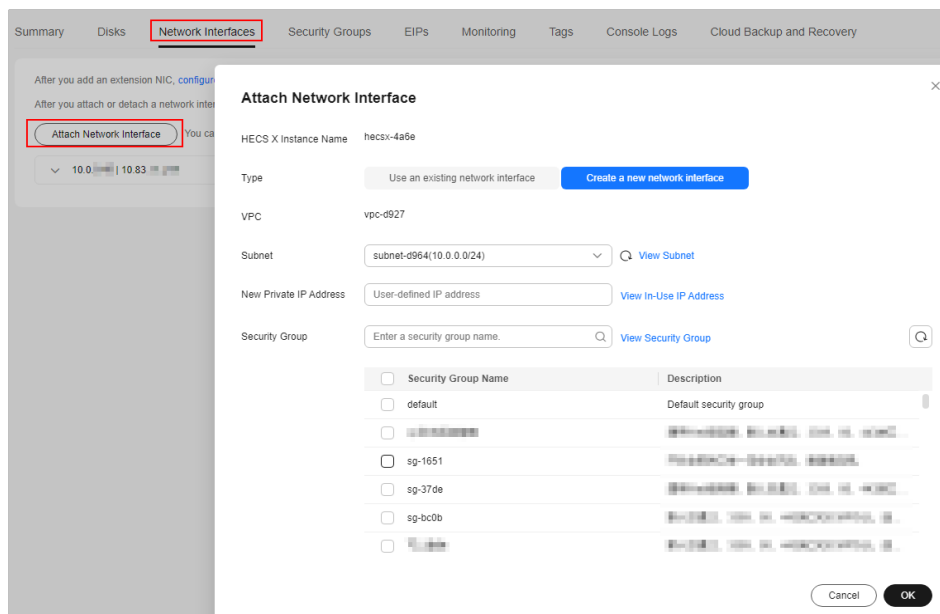
1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the target FlexusX instance and click its name.
The details page of this instance is displayed.
3. On the **Network Interfaces** tab, click **Attach Network Interface**.
You can use an existing extension network interface or create a new one.

Figure 2-5 Attaching an extension network interface

- **Subnet:** This parameter is mandatory. You need to select a subnet where the network interface will work.
- **New Private IP Address:** This parameter is optional. You can specify a private IP address for the network interface. If it is not specified, the system automatically assigns a private IP address.
- **Security Group:** This parameter is mandatory. You can select multiple security groups at a time. In this case, the rules of all the selected security groups are applied to the FlexusX instance.

4. Click **OK**.

Related Operations

After an extension network interface is attached to a FlexusX instance, it is recommended to enable NIC multi-queue to improve network performance. For details, see [Enabling NIC Multi-Queue](#).


2.7.3 Detaching Extended Network Interfaces

Scenarios

You can detach extension network interfaces from your FlexusX instance if they are no longer needed. Only extension network interfaces can be detached from the FlexusX instance. You cannot detach the primary network interface from it.

This section describes how to detach an extension network interface on the console.

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.

2. Locate the target FlexusX instance and click its name.
The details page of this instance is displayed.
3. On the **Network Interfaces** tab, choose **More > Detach**.

 **NOTE**

You are not allowed to delete the primary network interface from this instance. By default, the primary network interface is the first one in the list.

4. Click **OK** in the displayed dialog box.

 **NOTE**

Some FlexusX instances do not support network interface detachment when they are running. For details, see the GUI display. To detach a network interface from such a FlexusX instance, stop the instance first.

2.7.4 Changing a VPC

Scenarios

You can move your FlexusX instance from the current VPC to another.

Constraints

- Only running or stopped FlexusX instances support VPC change.
- The VPC of a FlexusX instance can be changed only if the instance has one network interface.
- If you have reinstalled or changed the OS of a FlexusX instance before changing the VPC, log in to the FlexusX instance and check whether the password or key pair configured during the reinstallation or change is successfully injected.
 - If the login is successful, the password or key pair is injected. Perform operations as required.
 - Otherwise, the system is injecting the password or key pair. During this period, do not perform any operations on the FlexusX instance.
- During the VPC switchover, do not bind, unbind, or change the EIP. Otherwise, a message will be displayed indicating insufficient permissions, but you do not need to take any action.
- If the network interface of a FlexusX instance has an IPv6 address, the VPC cannot be changed for the instance.

Notes

- A VPC can be changed on a running FlexusX instance, but the instance network connection will be interrupted during the change process.


 **NOTE**

If you intend to change the VPC for a running FlexusX instance, the VPC change may fail when traffic is being routed to the network interface of the instance. In this case, you are advised to try again later or stop the instance and try again.

- After the VPC is changed, the subnet, private IP address, MAC address, and OS network interface name of the FlexusX instance will change accordingly.

- After the VPC is changed, you need to reconfigure the source/destination check and the virtual IP address for the instance.
- After the VPC is changed, you need to reconfigure network-related application software and services, such as ELB, VPN, NAT Gateway, and DNS.

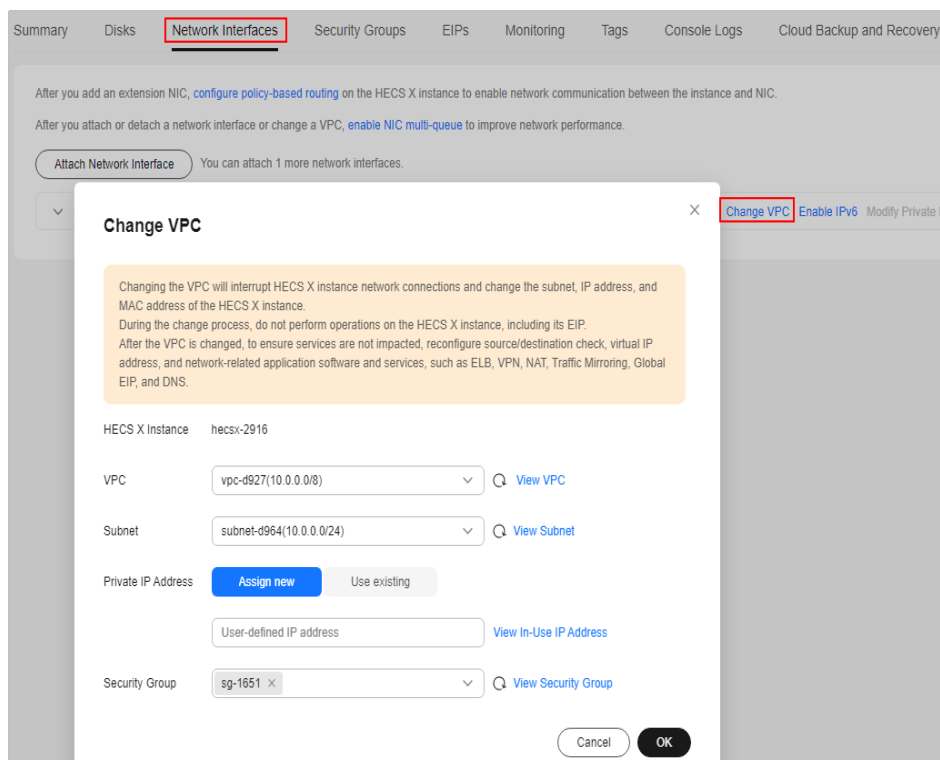
Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the target FlexusX instance and click its name.
The details page of this instance is displayed.
3. On the **Network Interfaces** tab, click **Change VPC**.
Select an available VPC and subnet from the drop-down list, and set the private IP address and security group as needed.
You can select multiple security groups. In this case, the rules of all the selected security groups are applied to the FlexusX instance.

NOTE

Using multiple security groups may deteriorate the network performance of a FlexusX instance. You are advised to select no more than five security groups.

Figure 2-6 Changing a VPC



4. Click **OK**.

2.7.5 Changing a Private IP Address


Scenarios

You can change the private IP address of the primary network interface for a FlexusX instance on the console.

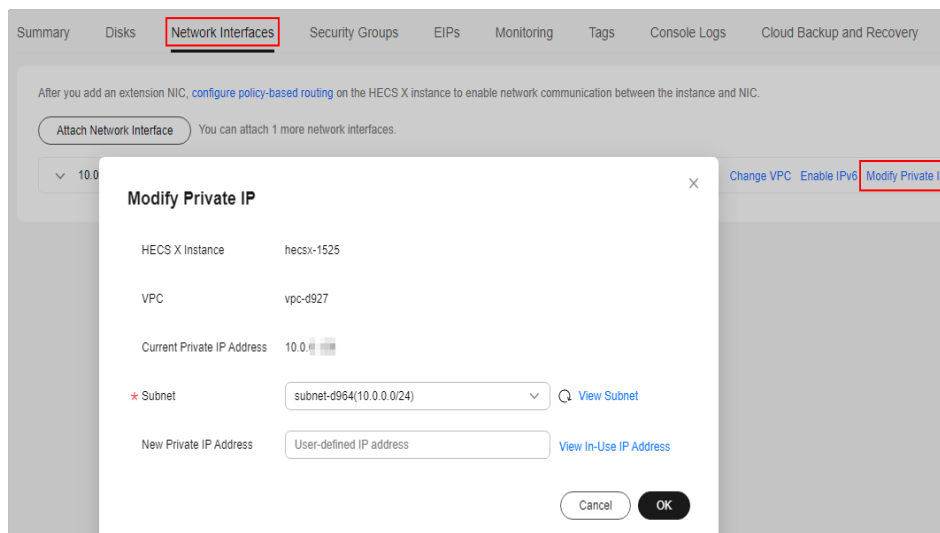
Notes and Constraints

- The FlexusX instance must be stopped.
- If a virtual IP address or DNAT rule has been configured for the network interface, cancel the configuration before modifying the private IP address.
- If the network interface has an IPv6 address, its private IPv4 or IPv6 address cannot be modified.
- To change the private IP address for a backend server of a load balancer, remove the backend server from the backend server group first.

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the target FlexusX instance and click its name.
The details page of this instance is displayed.
3. On the **Network Interfaces** tab, locate the primary network interface and click **Modify Private IP**.

The **Modify Private IP** dialog box is displayed.



4. Change the subnet and private IP address of the primary network interface as required.
 - **Subnet:** You can change the subnet when changing the private IP address.

NOTE

You can only change to a subnet within the same VPC.

- **New Private IP Address:** You can specify a new private IP address. If you do not specify a private IP address, the system will automatically assign one to the primary network interface.


2.7.6 Assigning a Virtual Private IP Address

Scenarios

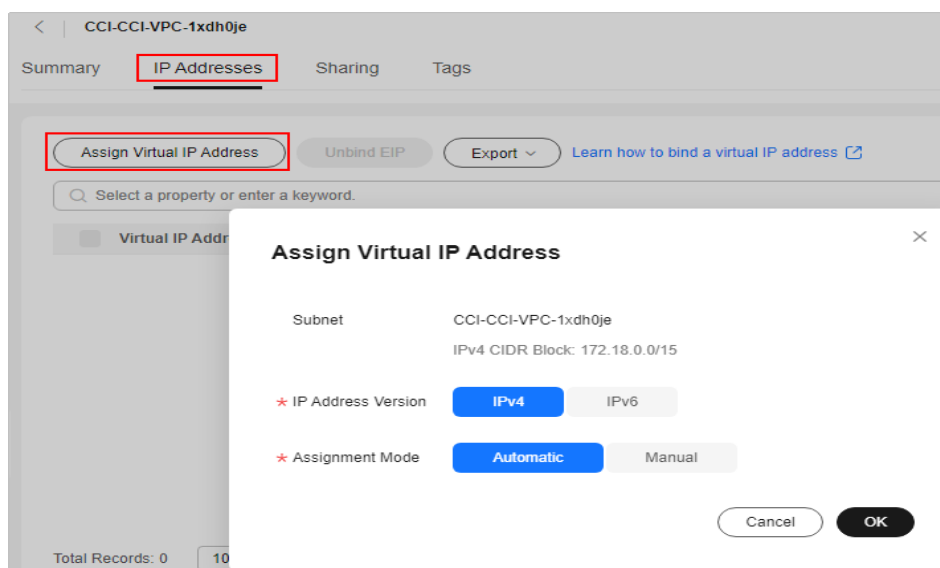
A virtual IP address serves as a secondary IP address for a network interface. A virtual IP address can be bound to multiple cloud servers to improve server availability.

If you want to use a virtual private IP address for a FlexusX instance, apply for a virtual IP address, bind the virtual IP address to the instance, and log in to the instance to manually configure the virtual IP address. This section describes how to use virtual IP addresses. For more information, see [Virtual IP Address Overview](#).

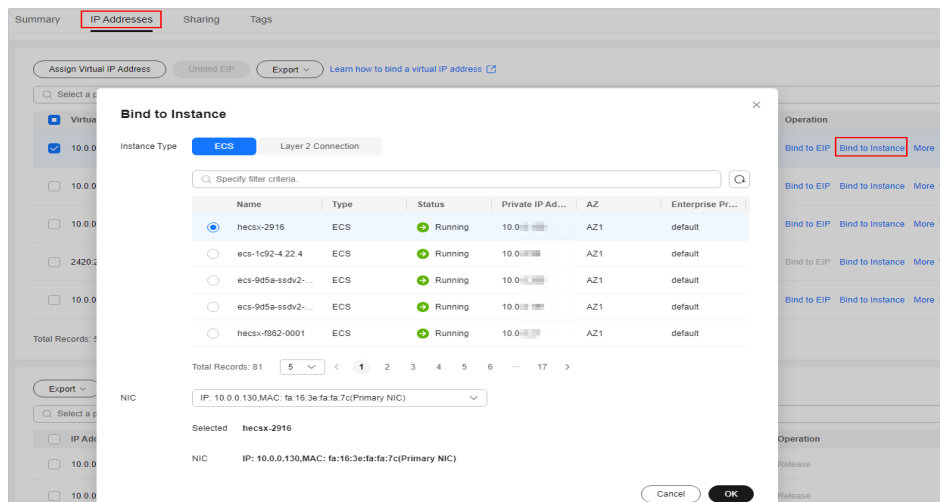
Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the target FlexusX instance and click its name.
The details page of this instance is displayed.
3. On the **Network Interfaces** tab, click **Manage Virtual IP Address**.
4. On the **IP Addresses** tab, click **Assign Virtual IP Address**, configure parameters, and click **OK**.

You can manually set a virtual IP address. If you do not specify one, the system will automatically assign a virtual IP address.



5. Click **Bind to Instance** in the **Operation** column of the target virtual IP address, select the server to be bound, and click **OK**.



Follow-Up Operations

After a virtual IP address is bound to the network interface of a FlexusX instance, you need to manually configure the virtual IP address bound to the instance. For details, see [Configuring a Virtual IP Address for an ECS](#).

2.8 Managing EIPs

2.8.1 Elastic IP Overview

What Is Elastic IP?

The Elastic IP (EIP) service enables your cloud resources to communicate with the Internet using static public IP addresses and scalable bandwidths. If a FlexusX instance has an EIP bound, it can directly access the Internet. If a FlexusX instance only has a private IP address, it cannot access the Internet. For details, see [What Is Elastic IP?](#)

Related Operations

Operation	Description	Reference
Binding an EIP	You can bind an EIP to a FlexusX instance so that the instance can access the Internet.	Binding an EIP
Unbinding an EIP	If your FlexusX X instance does not need to access the Internet or you want to change an EIP, you can unbind the EIP from the instance.	Unbinding an EIP
Changing an EIP	You cannot directly change the EIP of a FlexusX instance. To change the EIP, you can unbind the exiting EIP and bind a new one to the instance.	<ul style="list-style-type: none">Unbinding an EIPBinding an EIP

Operation	Description	Reference
Modifying a bandwidth	You can modify the name, billing mode, and size of a bandwidth.	Modifying a bandwidth
Releasing an EIP	After an EIP is unbound, it is still billed. If you no longer need the EIP, release it in a timely manner.	Releasing an EIP


2.8.2 Binding an EIP

Scenarios

You can assign an EIP and bind it to a FlexusX instance to enable the instance to access the Internet.

For details, see [Assigning an EIP and Binding It to an ECS](#).

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the target FlexusX instance, and in the **Operation** column, choose **More > Manage Network > Bind EIP**.
3. Bind an EIP.
 - **Select EIP:** Select an available EIP from the list. If no EIP is available in the current region, the EIP list is empty. In this case, assign an EIP and bind it to your instance.
 - **Release Option:** If you select **Release with FlexusX instance**, the EIP will be released when the FlexusX instance is deleted.




4. Click **OK**.
After an EIP is bound to the FlexusX instance, you can view the bound EIP.

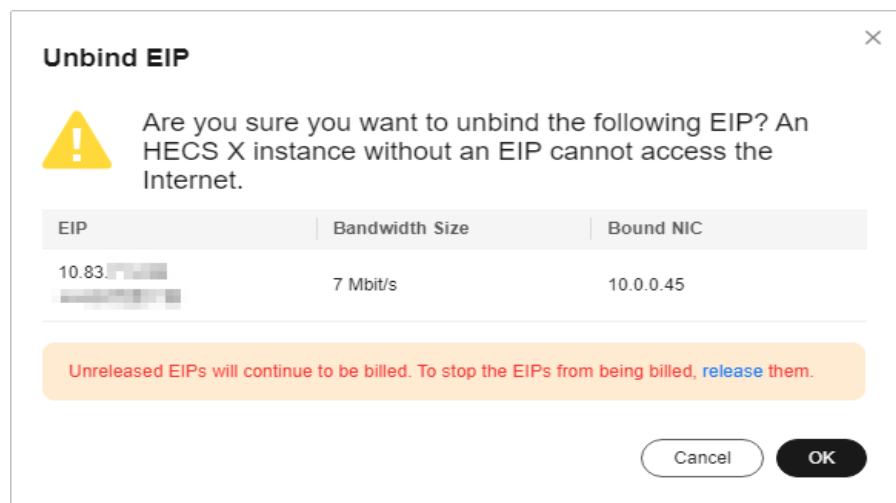
2.8.3 Unbinding an EIP

Scenarios

This section describes how to unbind an EIP from a FlexusX instance.

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the target FlexusX instance, and in the **Operation** column, choose **More > Manage Network > Unbind EIP**.
3. Confirm the EIP information and click **OK**.



NOTE

Unreleased EIPs will continue to be billed. Release them if you do not need them anymore.

2.8.4 Modifying a Bandwidth

Scenarios

If an EIP has been bound to a FlexusX instance, the instance can access the Internet using the bandwidth specified for the EIP. You can modify the name, billing mode, and size of a bandwidth. This section describes how to modify the bandwidth of a FlexusX instance.

The rule for modifying an EIP bandwidth depends on the billing mode of the EIP.

Table 2-5 Rules for modifying the bandwidth of EIPs in different billing modes

EIP Billing Mode	Billing Mode Changeable	Bandwidth Change	Billing Description
Yearly/ Monthly	No	<ul style="list-style-type: none"> • You can increase the bandwidth. The change is applied immediately. • You can decrease the bandwidth, but you need to renew the EIP, and the decreased bandwidth will take effect in the renewal period. For example, you purchased a FlexusX instance with a bandwidth of 5 Mbit/s in March and the required duration is one month. If you decrease the bandwidth to 2 Mbit/s and the renewal duration is one month, the bandwidth used in April will be 2 Mbit/s, but the bandwidth used in March is still 5 Mbit/s. 	<ul style="list-style-type: none"> • Increasing bandwidth The increased bandwidth will be billed accordingly. • Decreasing bandwidth The new bandwidth will be billed when the new subscription period starts.
Pay-per-use	Yes	You can increase or decrease the bandwidth. The changes are applied immediately.	Pay-per-use billing is a postpaid mode, so after the bandwidth is modified, you will be billed based on the new billing mode.

NOTE


- The yearly/monthly and pay-per-use billing modes in [Table 1](#) define how an EIP is billed, not how the FlexusX instance is billed.
Yearly/Monthly EIPs can only be billed by bandwidth, while pay-per-use EIPs can be billed by bandwidth, traffic, or shared bandwidth.
- When you purchase a yearly/monthly FlexusX instance, if you select **Traffic** or **Shared bandwidth** for **Billed By**, the EIP is billed on a pay-per-use basis. In this case, use the rules for modifying the bandwidth of a pay-per-use EIP.

The screenshot shows the 'EIP' configuration page. Under 'Purchase Mode', there are three buttons: 'Auto assign' (selected), 'Use existing', and 'Not required'. Under 'EIP Type', there is a button for '5_g-vm'. Under 'Billed By', there are three options: 'Bandwidth' (For heavy/stable traffic), 'Traffic' (For light/sharply fluctuating traffic), and 'Shared bandwidth' (For staggered peak hours). The 'Traffic' option is highlighted with a red box. Below the options, a note states: 'Billed based on total traffic irrespective of usage duration; configurable maximum bandwidth size.'

Notes and Constraints

- Modifying bandwidth is only available for FlexusX instances bound with EIPs.
- If a yearly/monthly EIP is bound to a FlexusX instance:
 - Only the bandwidth name and bandwidth size can be modified. A yearly/monthly EIP can only be billed by bandwidth.
 - The bandwidth size can be increased in the current subscription period, and decreased for the renewal period.
- Only the bandwidths of pay-per-use EIPs billed by bandwidth or traffic can be modified in batches. The bandwidths of yearly/monthly EIPs or pay-per-use EIPs billed by shared bandwidth cannot be modified in batches.

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Locate the FlexusX instance you want to modify the bandwidth for. Modify the bandwidth in either of the following ways:
 - In the **Operation** column of the FlexusX instance, choose **More > Manage Network > Modify Bandwidth**.
 - If the EIP bound to the FlexusX instance is billed by bandwidth or traffic, select the instance, and on the top of the list, choose **More > Modify Bandwidth**. You can use this method to modify bandwidth for such instances in batches.

The bandwidths of yearly/monthly EIPs or pay-per-use EIPs billed by shared bandwidth cannot be modified in batches.

3. Follow the instructions to modify the bandwidth.

Note

- The bandwidth name, size, and billing mode of an EIP whose billing mode is pay-per-use can be modified.
- If the bandwidth is billed by bandwidth size, specify a maximum bandwidth size and pay for the time for which you use the bandwidth. If the bandwidth is billed by traffic, you need to pay for the total traffic used regardless of the time for which you use the bandwidth.
- If you decrease the bandwidth, there may be some impact (such as packet loss) on running services.

Current Configuration

Bandwidth Name	bandwidth-1459	EIP	10.83.1.1
Bandwidth (Mbit/s)	7	Billed By	Traffic
Bandwidth Type	Dedicated		

New Configuration

* Bandwidth Name:

* Billed By: Bandwidth Traffic

* Bandwidth (Mbit/s): 1 2 5 10 100 200 Custom - 10 + The value ranges from 1 to 2,000 Mbit/s.

Parameter	Description
Billed By	<p>You can select Bandwidth or Traffic based on service requirements.</p> <ul style="list-style-type: none"> If you choose Bandwidth, you will be billed based on the new bandwidth size. If you choose Traffic, you will be billed based on the total amount of outbound traffic. The bandwidth size you set is only used to limit the maximum transfer rate. <p>NOTE A yearly/monthly EIP can only be billed by bandwidth.</p>
Bandwidth (Mbit/s)	<ul style="list-style-type: none"> Yearly/Monthly <ul style="list-style-type: none"> You can increase the bandwidth. The change is applied immediately. You can decrease the bandwidth, but you need to renew the EIP, and the decreased bandwidth will take effect in the renewal period. For example, you purchased a FlexusX instance with a bandwidth of 5 Mbit/s in March and the required duration is one month. If you decrease the bandwidth to 2 Mbit/s and the renewal duration is one month, the bandwidth used in April will be 2 Mbit/s, but the bandwidth used in March is still 5 Mbit/s. Pay-per-use You can increase or decrease the bandwidth. The changes are applied immediately.

4. Click **Next: Confirm**, confirm the information, and click **Submit**.

2.9 Managing Security Groups

2.9.1 Security Group

Overview

A security group is a collection of access control rules for cloud resources, such as cloud servers, containers, and databases, that have the same security protection requirements and that are mutually trusted. After a security group is created, you can configure access rules that will apply to all cloud resources added to this security group.

For more information about security groups, see [security groups](#).

NOTE

If two FlexusX instances are in the same security group but in different VPCs, the instances cannot communicate with each other. To enable communications between the two instances, connect the two VPCs first. For details, see [Connecting VPCs](#).

Security Group Rules

After a security group is created, you can add rules to the security group. A rule applies either to inbound traffic (ingress) or outbound traffic (egress). After FlexusX instances are added to the security group, they are protected by the rules of that group. For details about more configuration examples, see [Security Group Examples](#).

You can create a custom security group or use the default one provided by the system. The default security group permits all outbound traffic and denies inbound traffic. FlexusX instances in a security group can communicate with each other.

Table 2-6 Default security group rules

Direction	Action	Type	Protocol & Port	Source/ Destination	Description
Inbound	Allow	IPv4	All	Source: default security group (default)	Allows IPv4 instances in the security group to communicate with each other using any protocol over any port.
Inbound	Allow	IPv6	All		Allows IPv6 instances in the security group to communicate with each other using any protocol over any port.
Outbound	Allow	IPv4	All	Destination: 0.0.0.0/0	Allows access from instances in the security group to any IPv4 address over any port.
Outbound	Allow	IPv6	All	Destination: ::/0	Allows access from instances in the security group to any IPv6 address over any port.

Security Group Constraints

- By default, you can create up to 100 security groups in your cloud account.
- By default, you can add up to 50 rules to a security group.
- For better network performance, you are advised to associate no more than five security groups with a FlexusX instance or supplementary network interface.
- You can add up to 20 instances to a security group at a time.
- You can add up to 1,000 instances to a security group.


2.9.2 Configuring Security Group Rules

Scenarios

Similar to firewall, a security group is a logical group used to control network access. You can define access rules for a security group to protect the FlexusX instances that are added to this security group.

- Inbound rules allow or deny incoming network traffic to FlexusX instances in the security group.
- Outbound rules allow or deny outgoing network traffic from FlexusX instances in the security group.

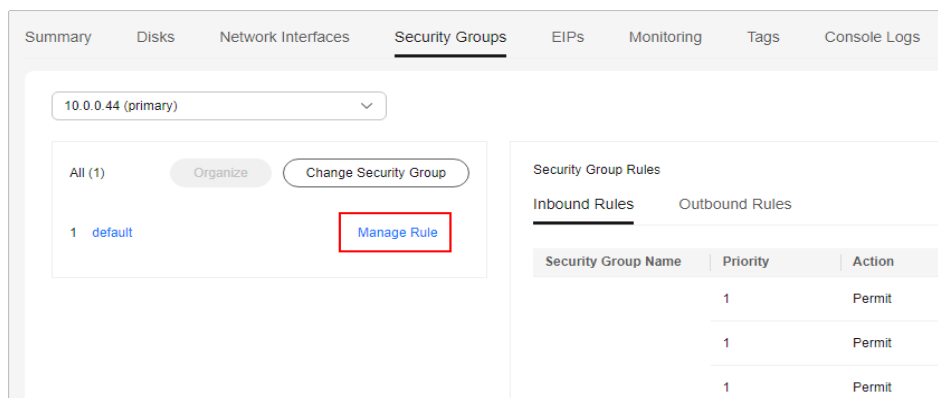
Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. On the **FlexusX Instances** page, locate the target FlexusX instance and click its name.

The details page of this instance is displayed.

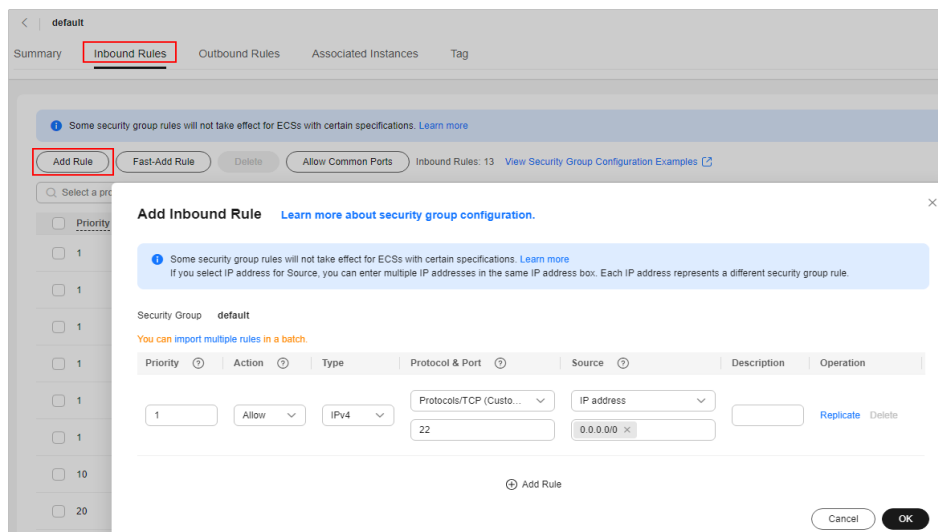
3. On the detailed page, click the **Security Groups** tab and view security group rules.
4. Click **Manage Rule**.

The page for configuring security group rules is displayed.



5. On the **Inbound Rules** tab, click **Add Rule**.
The **Add Inbound Rule** dialog box is displayed.
6. Configure required parameters.
You can click + to add more inbound rules. For details about the parameters, see [Adding a Security Group Rule](#).

Figure 2-7 Adding an inbound rule



7. On the **Outbound Rules** tab, click **Add Rule**.
The **Add Outbound Rule** dialog box is displayed.
8. Configure required parameters.
You can click + to add more outbound rules. For details about the parameters, see [Adding a Security Group Rule](#).
9. Click **OK**.

Verifying Security Group Rules

After adding inbound and outbound rules, you can verify whether the rules take effect. For example, if you have deployed a website on a FlexusX instance and want users to access your website through HTTP (80), you need to add an inbound rule to the security group to allow access over this port. [Table 2-7](#) shows the rule.

Table 2-7 The security group rule

Direction	Protocol/ Application	Port	Source
Inbound	TCP	80	0.0.0.0/0

Linux

If the instance runs Linux, perform the following operations to verify whether the security group rule is applied:

1. Log in to the FlexusX instance.
2. Run the following command to check whether TCP port 80 is listened on:
netstat -an | grep 80
If command output shown in **Figure 2-8** is displayed, TCP port 80 is listened on.

Figure 2-8 Command output for the Linux FlexusX instance

```
tcp        0      0 0.0.0.0:80          0.0.0.0:*        LISTEN
```

3. Enter **http://EIP bound to the FlexusX instance** in the address box of the browser and press **Enter**.
If the requested page can be accessed, the security group rule has taken effect.

Impacts of Deleting Common Security Group Rules

On the **Inbound Rules** and **Outbound Rules** tabs, you can also modify, replicate, or delete existing rules.

Deleting security group rules will disable some functions.


- If you delete a rule with **Protocol & Port** specified as **TCP: 20-21**, you will not be able to upload files to or download files from servers using FTP.
- If you delete a rule with **Protocol & Port** specified as **ICMP: All**, you will not be able to ping the servers.
- If you delete a rule with **Protocol & Port** specified as **TCP: 443**, you will not be able to connect to websites on the servers using HTTPS.
- If you delete a rule with **Protocol & Port** specified as **TCP: 80**, you will not be able to connect to websites on servers using HTTP.
- If you delete a rule with **Protocol & Port** specified as **TCP: 22**, you will not be able to remotely connect to Linux server using SSH.
- If you delete a rule with **Protocol & Port** specified as **TCP: 3389**, you will not be able to remotely connect to Windows server using RDP.

2.9.3 Changing a Security Group

Scenarios

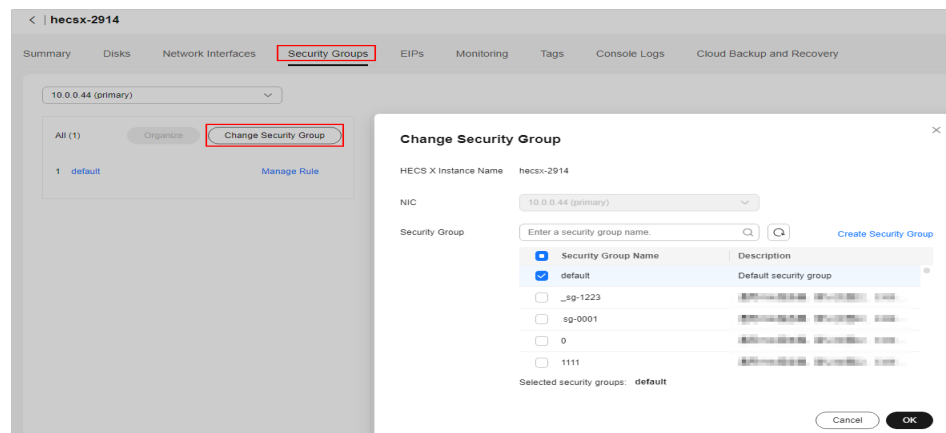
This section describes how to change the security group associated with the network interface of a FlexusX instance.

Procedure

1. Log in to the FlexusX **console**, click  in the upper left corner, and select a region and project.
2. On the **FlexusX Instances** page, locate the target FlexusX instance and click its name.
The details page of this instance is displayed.
3. On the **Security Groups** tab, click **Change Security Group**.

The **Change Security Group** dialog box is displayed.

Figure 2-9 Changing a security group



4. Select the target NIC and security groups.

You can select multiple security groups. In this case, the access rules of all the selected security groups are applied to the cloud server. To create a security group, click **Create Security Group**.

NOTE

Using multiple security groups may deteriorate the network performance of a FlexusX instance. You are recommended to select no more than five security groups.

5. Click **OK**.

2.10 Managing Server Security

What Is Host Security Service?

Host Security Service (HSS) helps you identify and manage the assets on your servers, 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.

After installing the HSS agent on your FlexusX instances, you will be able to check the protection status of the instances and risks in a region on the HSS console.

For more information about HSS, see [Host Security Service](#).

Enabling HSS

Before using the HSS service, install the agent on your FlexusX instance. You can install the agent during or after the creation of a FlexusX instance.

- **Scenario 1: During the creation of a FlexusX instance**

When you use certain public images to purchase FlexusX instances, you are advised to use HSS to protect your instances.

Select one of the following options:

- **HSS basic edition (free):** provides HSS basic edition (1-month free trial), account cracking protection, weak password detection, and malicious program detection.

 **NOTE**

After the free trial period expires, the HSS basic edition quotas will be automatically released, and HSS will not protect your servers.

If you want to retain or upgrade HSS security capabilities, you are advised to purchase HSS. For details, see [Editions and Features](#).

This option is selected by default.

- **Advanced HSS edition (paid):** provides HSS enterprise edition, vulnerability patches, virus scan and removal, and graded protection.
- **None:** Do not use security protection.

HSS provides basic, enterprise, premium, and WTP editions. For details, see [Edition Details](#).

If the basic or enterprise edition does not meet service requirements, you can [Purchasing an HSS Quota](#) and switch the edition on the HSS console to obtain advanced protection without reinstalling the agent.

 **NOTE**

Different public images support different HSS versions. See the supported HSS versions on the management console.


- **Scenario 2: After a FlexusX instance is purchased**

If you did not select **HSS** or the selected image does not support HSS when purchasing a FlexusX instance, you need to manually install the agent to use HSS.

For details, see [Installing an Agent](#) and [Enabling Server Protection](#).

Viewing the Security Status of FlexusX Instances

On the FlexusX instance list page, you can view the security of the instances.

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. In the FlexusX instance list, view the protection status of instances in the **Security** column.
 - **Not installed:** The agent is not installed, or the agent is installed but not enabled. If you want to install the agent, refer to [Installing an Agent](#).
(The security status of a newly purchased FlexusX instance may be **Agent not installed**, which is because the agent is being installed. Please check it later.)
 - **Risky:** The FlexusX instance is risky.
 - **Safe:** No risk is found in the FlexusX instance.
 - **Unprotected:** HSS is not enabled for the FlexusX instance. For details about how to enable HSS, see [Enabling Server Protection](#).
If HSS is not enabled on the newly purchased FlexusX instance, please manually install the Agent.

3. Click the name of the target FlexusX instance. The details page of this instance is displayed.
Select **HSS** to view the agent status and protection status.

2.11 Managing Server Monitoring

2.11.1 Overview

What Is Server Monitoring?

Monitoring is key for ensuring FlexusX instance performance, reliability, and availability. Using monitoring data, you can determine how well your FlexusX instance resources are used. The cloud platform provides Cloud Eye to help you obtain the statuses of your cloud servers. You can use Cloud Eye to automatically monitor cloud servers in real time and manage alarms and notifications to keep track of cloud server performance metrics.

Server monitoring consists of basic monitoring, OS monitoring, and process monitoring for servers.

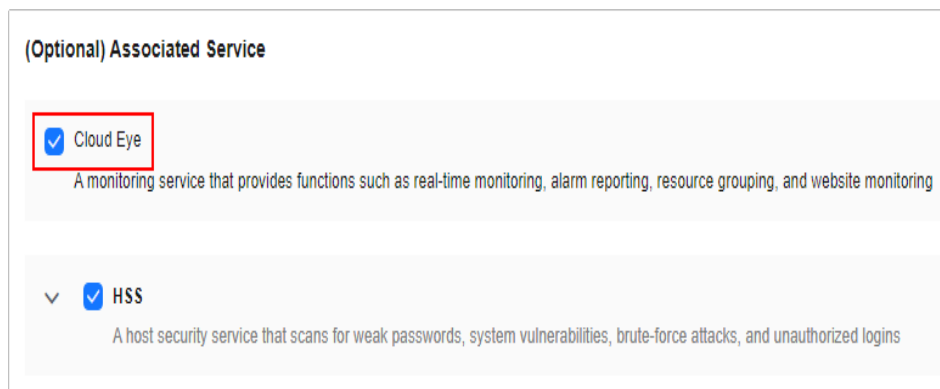
- Basic monitoring monitors metrics automatically reported by FlexusX instances, such as CPU usage.
- OS monitoring provides proactive, fine-grained OS monitoring for FlexusX instances, and it requires the Agent to be installed on all FlexusX instances to be monitored.
- Process monitoring monitors active processes on FlexusX instances, and it requires the Agent to be installed on the FlexusX instances to be monitored. By default, Cloud Eye collects CPU usage, memory usage, and the number of opened files of active processes.

Enabling Monitoring

On the FlexusX instance purchase page, you can choose whether to use Cloud Eye. No matter whether you use Cloud Eye, after the FlexusX instance is created, basic monitoring is offered for your instance by default. On the FlexusX instance purchase page:

- If you select Cloud Eye, you will be able to view basic monitoring, OS monitoring, and process monitoring data on the FlexusX console. The OS monitoring and process monitoring data can be viewed only after the **Agent** is installed.

Figure 2-10 Selecting Cloud Eye



- If you do not select Cloud Eye, you will be able to only view basic monitoring data on the FlexusX console.

If you want to view OS monitoring or process monitoring data, install the [Agent](#), and then view the OS monitoring or process monitoring data on the Cloud Eye console.

Related Operations

Operation	Description
Configuring an Alarm Rule	After monitoring is enabled, you can set alarm rules to receive notifications in a timely manner.
Viewing Server Monitoring Metrics	You can view FlexusX instance metrics after the FlexusX instances receive the monitoring data. You can view monitoring data on the FlexusX instance console or on the Server Monitoring page of the Cloud Eye console.

Helpful Links

- [Why Is My Linux ECS Running Slowly?](#)


2.11.2 Configuring an Alarm Rule

Scenarios

Configuring alarm rules for FlexusX instances allows you to customize the monitored objects and notification policies so that you can closely monitor your FlexusX instances.

This section describes how to configure an alarm rule for a FlexusX instance.

Configuring an Alarm Rule on the Cloud Eye Console

1. Log in to the [Cloud Eye console](#).
2. Click  in the upper left corner and select the desired region and project.
3. In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
4. On the **Alarm Rules** page, click **Create Alarm Rule** to create one, or modify an existing alarm rule.
 - [Creating an Alarm Rule](#)
 - [Modifying an Alarm Rule](#)

After an alarm rule is configured, the system automatically notifies you when an alarm complying with the alarm rule is generated.

NOTE

For more information about alarm rules, see [Introduction to Alarm Rules](#).

2.11.3 Viewing Server Monitoring Metrics

Scenarios

The cloud platform provides Cloud Eye to help you monitor FlexusX instances. You can view the metrics of each FlexusX instance on the management console.


Prerequisites

- The FlexusX instance is running properly.
Cloud Eye does not display the monitoring data for a stopped, faulty, or deleted FlexusX instance. After such a FlexusX instance restarts or recovers, the monitoring data is available on Cloud Eye.

NOTE

- Cloud Eye discontinues monitoring FlexusX instances that remain in the **Stopped** or **Faulty** state for 24 hours and removes them from the monitoring list. However, the alarm rules configured for such FlexusX instances are not automatically deleted.
- Alarm rules have been configured on Cloud Eye for the target FlexusX instance.
The monitoring data is unavailable for the FlexusX instances without alarm rules configured on Cloud Eye. For details, see [Configuring an Alarm Rule](#).
- The target FlexusX instance has been running for at least 10 minutes.
The monitoring data and graphs are available for a new instance after the instance runs for at least 10 minutes.

Procedure

1. Log in to the FlexusX [console](#), click  in the upper left corner, and select a region and project.
2. Click the name of the target FlexusX instance.
3. Click the **Monitoring** tab to view the monitoring data.

In the FlexusX instance monitoring area, select a duration to view the monitoring data.

It takes a period of time to transmit and display monitoring data. The monitoring data displayed was generated 5 to 10 minutes before the current time. You can view the monitoring data of a newly created FlexusX instance 5 to 10 minutes later.

3 FlexusRDS

3.1 Buying a FlexusRDS Instance

Scenarios

This section describes how to purchase a FlexusRDS instance on the management console.

FlexusRDS only supports the yearly/monthly billing mode. It allows you to tailor your compute resources and storage space to your business needs.

Prerequisites

- You have [created a Huawei ID and enabled Huawei Cloud services](#).
- Your account balance is greater than or equal to \$0 USD.

Procedure

Step 1 Go to the [FlexusRDS console](#).

Step 2 If this is your first time to create a FlexusRDS instance, click **Buy**.

Step 3 Configure the instance information and click **Buy**.

Figure 3-1 Selecting an instance class

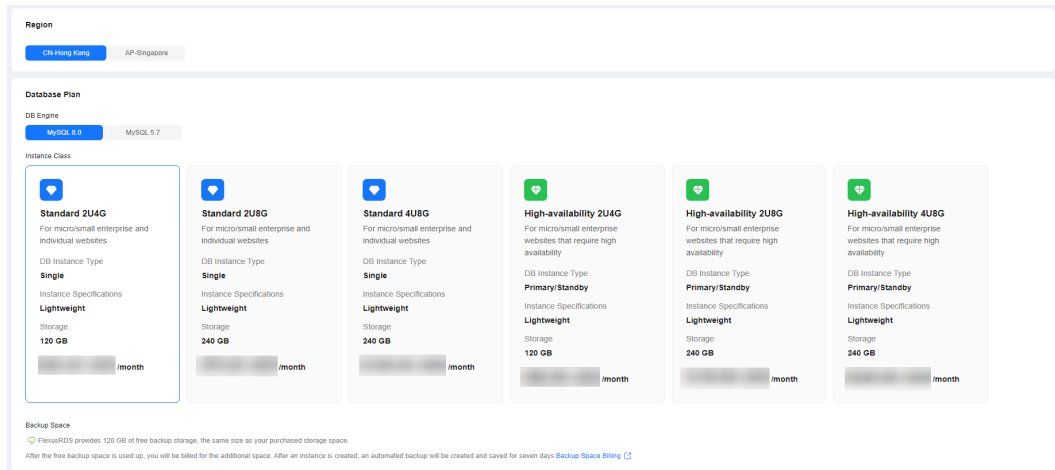


Figure 3-2 Selecting the required duration

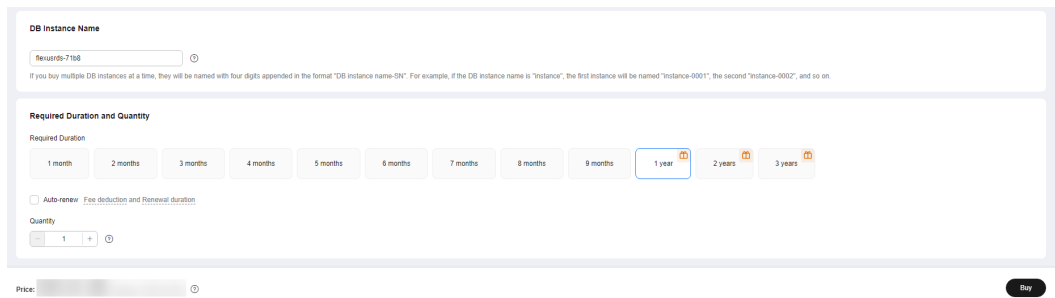
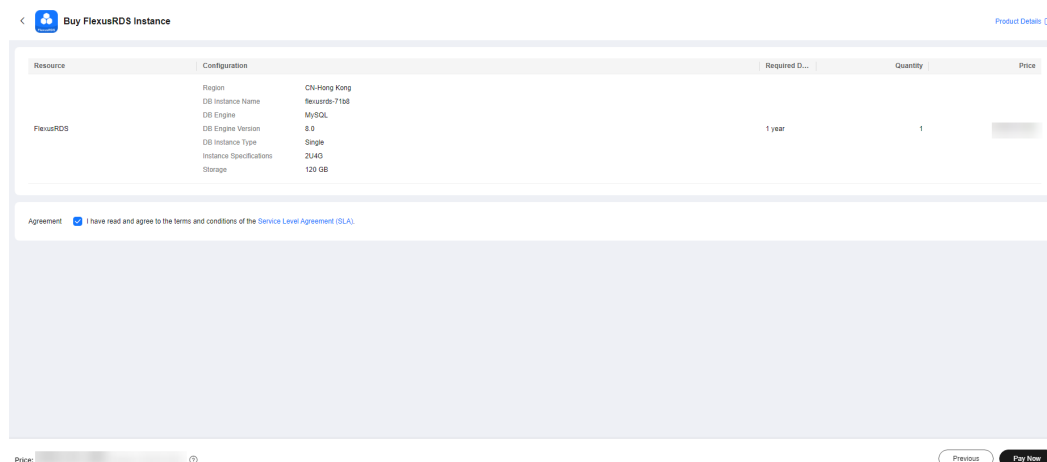


Table 3-1 Basic information

Parameter	Description
Region	Region where your resources are located. NOTE Available regions: CN-Hong Kong and AP-Singapore Products in different regions cannot communicate with each other through a private network. After a DB instance is created, the region cannot be changed. Therefore, exercise caution when selecting a region.
DB Engine	MySQL 8.0 and MySQL 5.7

Parameter	Description
Instance Class	<p>An instance class includes vCPUs, memory, storage, and DB instance type.</p> <ul style="list-style-type: none">• Storage: The purchased storage space. After a DB instance is purchased, you can configure storage autoscaling. The maximum allowed storage is 4,000 GB. For details, see Storage Autoscaling.• DB Instance Type<ul style="list-style-type: none">- Primary/Standby: uses an HA architecture with a primary DB instance and a synchronous standby DB instance. The standby DB instance improves instance reliability and is invisible to you after being created.- Single: uses a single-node architecture, which is less expensive than primary/standby DB instances.
DB Instance Name	<p>Must start with a letter and consist of 4 to 64 characters. Only letters (case-sensitive), digits, hyphens (-), underscores (_), and periods (.) are allowed.</p> <p>If you buy multiple DB instances at a time, they will be named <i>instance-0001</i>, <i>instance-0002</i>, and so on. (<i>instance</i> indicates the DB instance name you specify.)</p>
Required Duration	<p>The system will automatically calculate the configuration fee based on the selected required duration. The longer the required duration is, the larger discount you will enjoy.</p>
Auto-renew	<ul style="list-style-type: none">• This option is not selected by default.• If you select this option, the auto-renew cycle is determined by the selected required duration.
Quantity	<p>You can buy a maximum of 50 DB instances at a time. If you intend to create primary/standby DB instances and set Quantity to 1, a primary instance and a synchronous standby instance will be created.</p>

Step 4 Confirm the order.

Figure 3-3 Order confirmation

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Pay Now**.

Step 5 Select a payment method and complete the payment.

Step 6 To view and manage your instance, go to the instance list page.

- When your instance is being created, the status is **Creating**. The status changes to **Available** after the instance is created.
- Automated backup is enabled by default during instance creation. An automated full backup is immediately triggered once your DB instance is created.
- The default administrator account of your DB instance is **root**.
- During instance creation, the system randomly sets a password for the administrator account. You need to **reset the password** before you can connect to the instance.
- The default database port is **3306** and cannot be changed.
- The VPC, subnet, and security group to which the instance belongs are **vpc-default-smb**, **subnet-default-smb**, and **sg-default-smb** by default and cannot be changed.

----End

3.2 Connecting to a FlexusRDS Instance

3.2.1 Using DAS to Connect to a FlexusRDS Instance (Recommended)

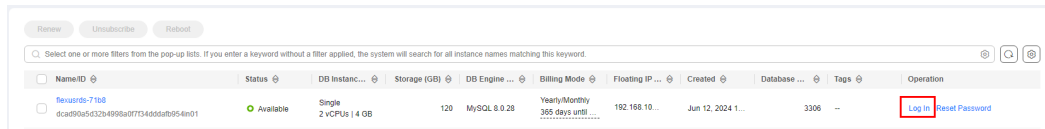
Scenarios

Data Admin Service (DAS) enables you to connect to and manage DB instances with ease on a web-based console. The permission required for connecting to DB instances through DAS has been enabled for you by default. Using DAS to connect to your DB instance is recommended, which is more secure and convenient.

Procedure

- Step 1** In the instance list, locate the target DB instance and click **Log In** in the **Operation** column.

Figure 3-4 Logging in to an instance



Alternatively, click the instance name in the instance list. On the displayed page, click **Log In** in the upper right corner.

- Step 2** On the displayed login page, enter the username and password and click **Log In**.
----End

3.2.2 Using CLI to Connect to a FlexusRDS Instance

Scenarios

You can connect to your DB instance using the MySQL command-line interface (CLI) from a FlexusX instance with a MySQL client installed.

FlexusX instances and FlexusRDS instances in the same region are in the same VPC, subnet, and security group by default and can communicate with each other.

Procedure

- Step 1** [Log in to the FlexusX instance in the same region as your FlexusRDS DB instance.](#)
- Step 2** Download the MySQL client installation package for Linux to the FlexusX instance. The package `mysql-community-client-5.7.38-1.el6.x86_64.rpm` is used as an example.

```
wget https://dev.mysql.com/get/mysql-community-client-5.7.38-1.el6.x86_64.rpm
```

NOTE

A MySQL client running a version later than that of the FlexusRDS DB instance is recommended.

- Step 3** Install the MySQL client.

```
rpm -ivh --nodeps mysql-community-client-5.7.38-1.el6.x86_64.rpm
```

 NOTE

- If any conflicts occur during the installation, add the **replacefiles** parameter to the command and install the client again.
rpm -ivh --replacefiles mysql-community-client-5.7.38-1.el6.x86_64.rpm
- If a message is displayed prompting you to install a dependent package during the installation, add the **nodeps** parameter to the command and install the client again.
rpm -ivh --nodeps mysql-community-client-5.7.38-1.el6.x86_64.rpm

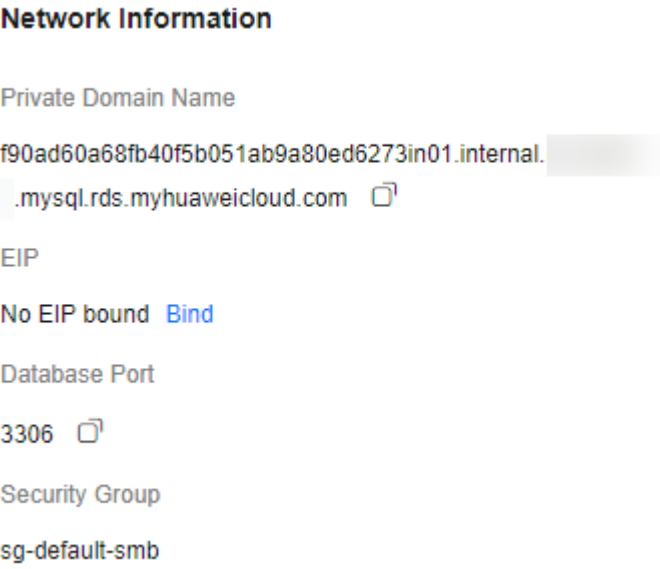
Step 4 Run the following command on the FlexusX instance to connect to the FlexusRDS DB instance:

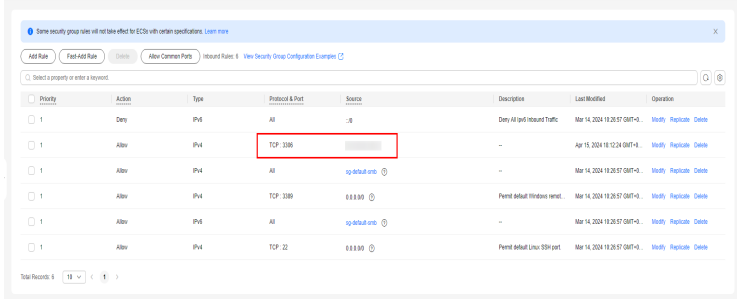
```
mysql -h <host> -P <port> -u <userName> -p
```

Example:

```
mysql -h 192.168.0.1 -P 3306 -u root -p
```

Table 3-2 Parameter description

Parameter	Description
<host>	<p>The DB instance to be connected. You can connect to your DB instance over a private network or public network. For higher security, private network connection is recommended.</p> <ul style="list-style-type: none"> Private network connection (recommended): Click the DB instance name and obtain the private domain name on the Overview page. Public network connection: Click the DB instance name and obtain the EIP on the Overview page. For details about how to bind an EIP to a DB instance, see Binding and Unbinding an EIP. <p>Figure 3-5 Network information</p>  <p>The screenshot shows the following information:</p> <ul style="list-style-type: none"> Network Information Private Domain Name: f90ad60a68fb40f5b051ab9a80ed6273in01.internal. [redacted].mysql.rds.myhuaweicloud.com EIP: No EIP bound Bind Database Port: 3306 Security Group: sg-default-smb <p>To connect to your DB instance through an EIP, add the EIP and port 3306 to an inbound rule of security group sg-default-smb. For details, see Adding a Security Group Rule.</p>

Parameter	Description
	<p>Figure 3-6 Adding an inbound rule</p> 
<port>	3306
<userName>	root

Step 5 When the following information is displayed, enter the password of user **root**:
Enter password:

----End

3.3 Managing FlexusRDS Instances

3.3.1 Suggestions on Using FlexusRDS

3.3.1.1 Instance Usage Suggestions

DB Instances

- Primary/Standby
 - A primary/standby pair provides an HA architecture.
 - When a primary instance is being created, a standby instance is provisioned along with it to provide data redundancy. The standby instance is invisible to you after being created.
 - If a failover occurs due to a primary instance failure, your database client will be disconnected for a short period of time. The client needs to be able to reconnect to the instance.
- Single
 - A single-node architecture is used.
 - If a fault occurs on a single instance, the instance cannot recover in a timely manner.

Database Connection

- Set database parameters based on the complexity of your workloads.

- Keep an appropriate number of active connections.
- Periodically release persistent connections because maintaining them may generate a large cache and use up memory.

Reliability and Availability

- Select primary/standby DB instances for production databases.
- Select an instance class and storage space appropriate to your workloads.

Backup and Restoration

- To prevent backup failures, perform manual backups during off-peak hours.
- Both automated and manual backups are deleted after your instance is unsubscribed from.

Routine O&M

- Periodically check slow query logs and error logs to identify problems in advance.
- Monitor instance metrics. If any metric is beyond its expected range, address related issues as soon as possible.
- Run the **SELECT** statement before deleting or modifying a record.

Security

- Prevent your instance from being accessed from the Internet. If you want to allow the access from the Internet, bind an EIP to your instance.

3.3.1.2 Database Usage Suggestions

Database Naming

- The names of database objects like databases, tables, and columns should be in lowercase. Different words in the name are separated with underscores (_).
- Reserved words and keywords cannot be used to name database objects in FlexusRDS.
 - Reserved words and keywords for MySQL 8.0: <https://dev.mysql.com/doc/refman/8.0/en/keywords.html>
 - Reserved words and keywords for MySQL 5.7: <https://dev.mysql.com/doc/refman/5.7/en/keywords.html>
- Each database object name must be explainable and contain a maximum of 32 characters.
- Each temporary table in databases is prefixed with **tmp** and suffixed with a date.
- Each backup table in databases is prefixed with **bak** and suffixed with a date.
- All columns storing the same data in different databases or tables must have the same name and be of the same type.

Database Design

- All tables use the InnoDB storage engine unless otherwise specified. InnoDB supports transactions and row locks. It delivers excellent performance, making it easy to recover data.
- Databases and tables all use the UTF8 character set to avoid characters getting garbled by character set conversion.
- All tables and fields require comments that can be added using the COMMENT clause to maintain the data dictionary from the beginning of the design.
- The length of a single row in the table cannot exceed 1024 bytes.
- To avoid cross-partition queries, FlexusRDS partitioned tables are not recommended. Cross-partition queries will decrease the query efficiency. A partitioned table is logically a single table, but the data is actually stored in multiple different files.
- Do not create too many columns in one table. Store cold and warm data separately to reduce the width of a table. In doing so, more rows of data can be stored in each memory page, decreasing disk I/O and making more efficient use of the cache.
- Columns that are frequently used together should be in the same table to avoid JOIN operations.
- Do not create reserved fields in a table. Otherwise, modifying the column type will lock the table, which has a greater impact than adding a field.
- Do not store binary data such as images and files in databases.
- Full-text indexes are not recommended because there are many limitations on full-text indexes for MySQL Community Edition.

Field Design

- Ensure that each table contains no more than 50 fields.
- Select a small data type for each column as much as possible. Numeric data is preferred, followed by dates or binary data, and the least preferred is characters. The larger the column data type, the more the space required for creating indexes. As a result, there are fewer indexes on a page and more I/O operations required, so database performance deteriorates.
- If the integer type is used as the database field type, select the shortest column type. If the value is a non-negative number, it must be the unsigned type.
- Each field should have the NOT NULL attribute. The default value for the numeric type such as INT is recommended to be 0, and that for the character type such as VARCHAR is recommended to be an empty string.
- Do not use the ENUM type. Instead, use the TINYINT type.
Change ENUM values using ALTER. The ORDER BY operations on ENUM values are inefficient and require extra operations.
If you have specified that ENUM values cannot be numeric, other data types (such as char) can be used.
- If the numeric data type is required, use DECIMAL instead of FLOAT or DOUBLE.

FLOAT and DOUBLE data cannot be stored precisely, and value comparison results may be incorrect.

- When you want to record a date or specific time, use the DATETIME or TIMESTAMP type instead of the string type.
- Store IP addresses using the INT UNSIGNED type. You can convert IP addresses into numeric data using function inet_aton or inet_ntoa.
- The VARCHAR data should be as short as possible. Although the VARCHAR data varies in length dynamically on disks, it occupies the maximum length in memory.
- Use VARBINARY to store variable-length character strings that are case-sensitive. VARBINARY is case-sensitive by default and quick to process because no character sets are involved.

Index Design

- Create a primary key for each InnoDB table. Neither use a frequently-updated column as the primary key nor a multi-column primary key. Do not use the UUID, MD5, or character string column as the primary key. Use a column whose values can increment continuously as the primary key. So, the auto-increment ID column is recommended.
- Use no more than 5 indexes in a single table. Indexes speed up queries, but too many indexes may slow down writes. Inappropriate indexes sometimes reduce query efficiency.
- Do not create an independent index for each column in a table. A well-designed composite index is much more efficient than a separate index on each column.
- Create an index on the following columns:
 - Columns specified in the WHERE clause of SELECT, UPDATE, or DELETE statements
 - Columns specified in ORDER BY, GROUP BY, or DISTINCT
 - Columns associated for joining multiple tables.
- The index column order is as follows:
 - Put the column with the highest selectivity on the far left when creating a composite index. $\text{Selectivity} = \frac{\text{Different values in a column}}{\text{Total rows in the column}}$
 - Put the column with the smallest field length on the far left of the composite index. The smaller length a field has, the more data one page stores, and the better the I/O performance is.
 - Put the most frequently used column on the left of the composite index, so you can create fewer indexes.
- Avoid using redundant indexes, such as primary key (id), index (id), and unique index (id).
- Avoid using duplicate indexes, such as index(a,b,c), index(a,b), and index(a). Duplicate and redundant indexes may slow down queries because the FlexusRDS query optimizer does not know which index it should use.
- When creating an index on the VARCHAR field, specify the index length based on selectivity. Do not index the entire field.

If an index with the length of 20 bytes is the string type, its selectivity can reach 90% or above. In this case, use **count(distinct left(column name, index length))/count(*)** to check index selectivity.

- Use covering indexes for frequent queries.
A covering index is a special type of index where all required fields for a query are included in the index. The index itself contains columns specified in WHERE and GROUP BY clauses, but also column combinations queried in SELECT, without having to execute additional queries.
- Constraints on foreign keys are as follows:
The character sets of the columns for which a foreign key relationship is established must be the same, or the character sets of the parent and child tables for which a foreign key relationship is established must be the same.

SQL Statement Development

- Use prepared statements to perform database operations in programs. Prepared statements can be executed multiple times in a program once they are written, more efficient than SQL statements.
- Avoid implicit conversions because they may cause index to become invalid. Do not perform function conversions or math calculations on columns in the WHERE clause. Otherwise, the index becomes invalid.
- Do not use double percent signs (%%) or place % before a query condition, or the index cannot be used.
- Do not use **select *** for queries because using **select ***:
 - Consumes more CPUs, IP addresses, and bandwidth.
 - Causes covering indexes to become unavailable.
 - Increases the impact of table structure changes on code.
- Do not use subqueries. Subqueries generate temporary tables that do not have any indexes. If there is a lot of data, the query efficiency is severely affected. Convert subqueries into associated queries.
- Minimize the use of JOIN operations for more than five tables. Use the same data type for the fields that require JOIN operations.
Each JOIN operation on a table occupies extra memory (controlled by **join_buffer_size**) and requires temporary table operations, affecting query efficiency. Do not use NATURAL JOIN.
- Reduce interactions with the same database as much as possible. The database is more suitable for processing batch operations.
- Replace OR operations with IN operations. IN operations can effectively use indexes. The number of IN values cannot exceed 500.
- Do not perform reverse queries, for example, NOT IN and NOT LIKE.
- Do not use ORDER BY RAND() for random sorting.
This operation loads all data that meets the conditions from the table to the memory for sorting, consuming more CPUs, I/O, and memory resources.
Obtain a random value from the program and retrieve data from the involved database based on the value.
- If deduplication is not required, use UNION ALL instead of UNION.
UNION ALL does not sort out result sets.

- Combine multiple operations and perform them in batches. The database is good for batch processing.
This reduces interactions with the same database.
- If there are more than 1 million rows of write operations, perform them in multiple batches.
A large number of batch writes may result in excessive primary/standby latency.
- If ORDER BY is used, use the order of indexes.
 - The last field of ORDER BY is a part of a composite index and is placed at the end of the composite index order.
 - Avoid file_sort to speed up queries.
Correct example: in **where a=? and b=? order by c;**, index: **a_b_c**
Wrong example: If an index supports range search, the index order cannot be used. For example, **WHERE a>10 ORDER BY b;**, index: **a_b** (sorting is not allowed)
- Use ANSI-standard SQL statements instead of MySQL extended SQL statements for DML operations. Common MySQL extended SQL statements include:
 - REPLACE INTO
 - INSERT ... ON DUPLICATE KEY UPDATE
- Stored procedures are not recommended because they are difficult to debug, extend, and transplant.
- To avoid logical dependency on the database, do not use triggers, event schedulers, or views for service logic.
- Large transactions are not recommended. If possible, a transaction should contain no more than five SQL statements because large transactions have problems such as long data lock time, too many caches, and connection consumption.
- TRUNCATE TABLE is faster than DELETE and uses fewer system and log resources. If the table to be deleted does not have a trigger and the entire table needs to be deleted, TRUNCATE TABLE is recommended.
- Do not run the **flush logs** command frequently to prevent automatic binlog deletion failures.

3.3.2 Database Migration

3.3.2.1 Migrating Data to FlexusRDS Using mysqldump

Preparing for Data Migration

You can access your FlexusRDS DB instance through an EIP or from a FlexusX instance.

1. Prepare a FlexusX instance for accessing your FlexusRDS DB instance or prepare a device for accessing your FlexusRDS DB instance through an EIP.
To connect to a FlexusRDS instance through an EIP, **bind an EIP** to the instance.

2. Install a MySQL client of the same version as your FlexusRDS instance on the prepared FlexusX instance or device.

NOTE

A MySQL client will provide `mysqldump` and `mysql`.
MySQL system databases `mysql` and `sys` cannot be imported to FlexusRDS instances.

Exporting Data

Before migrating a database to FlexusRDS, its data needs to be exported.

NOTICE

- The export tool must match the DB engine version.
- Database migration is performed offline. Before the migration, you have to stop all applications using the source database.

Step 1 Log in to the source database.

Step 2 Use the `mysqldump` tool to export the table structure to an SQL file.

NOTICE

The `mysql` database is required for FlexusRDS management. When exporting the table structure, do not specify `--all-database`. Otherwise, a database fault will occur.

```
mysqldump--databases<DB_NAME>--single-transaction --order-by-primary --hex-blob --no-data --routines --events --set-gtid-purged=OFF-u <DB_USER>-p -h<DB_ADDRESS>-P <DB_PORT>|sed -e 's/DEFINER[ ]*=[ ]*[^\]*\*/' -e 's/DEFINER[ ]*.*FUNCTION/FUNCTION/' -e 's/DEFINER[ ]*.*PROCEDURE/PROCEDURE/' -e 's/DEFINER[ ]*.*TRIGGER/TRIGGER/' -e 's/DEFINER[ ]*.*EVENT/EVENT/' ><BACKUP_FILE>
```

- `DB_NAME` indicates the name of the database to be migrated.
- `DB_USER` indicates the database username.
- `DB_ADDRESS` indicates the database address.
- `DB_PORT` indicates the database port.
- `BACKUP_FILE` indicates the name of the file to which the data will be exported.

Enter the database password when prompted.

Example:

```
mysqldump --databases frdsdb --single-transaction --order-by-primary --hex-blob --no-data --routines --events --set-gtid-purged=OFF -u root -p -h 192.168.151.18 -P 3306 |sed -e 's/DEFINER[ ]*=[ ]*[^\]*\*/' -e 's/DEFINER[ ]*.*FUNCTION/FUNCTION/' -e 's/DEFINER[ ]*.*PROCEDURE/PROCEDURE/' -e 's/DEFINER[ ]*.*TRIGGER/TRIGGER/' -e 's/DEFINER[ ]*.*EVENT/EVENT/' > dump-defs.sql
```

Enter password:

After this command is executed, a **dump-defs.sql** file will be generated as follows:

```
[rds@localhost ~]$ ll dump-defs.sql
-rw-r-----. 1 rds rds 2714 Sep 21 08:23 dump-defs.sql
```

Step 3 Use the mysqldump tool to export data to an SQL file.

NOTICE

The **mysql** database is required for FlexusRDS management. When exporting data, do not specify **--all-database**. Otherwise, a database fault will occur.

```
mysqldump --databases<DB_NAME>--single-transaction --hex-blob --set-gtid-purged=OFF --no-create-info --skip-triggers-u<DB_USER>-p-h<DB_ADDRESS>-P<DB_PORT>-r<BACKUP_FILE>
```

For details on the parameters in the preceding command, see [2](#).

Enter the database password when prompted.

Example:

```
mysqldump --databases frdsdb --single-transaction --hex-blob --set-gtid-purged=OFF --no-create-info --skip-triggers -u root -p -h 192.168.151.18 -P 3306 -r dump-data.sql
```

After this command is executed, a **dump-data.sql** file will be generated as follows:

```
[rds@localhost ~]$ ll dump-data.sql
-rw-r-----. 1 rds rds 2714 Sep 21 08:23 dump-data.sql
```

----End

Importing Data

You can connect your client to the FlexusRDS instance and import exported SQL files into it.

NOTICE

If the source database calls triggers, stored procedures, functions, or events, you must set **log_bin_trust_function_creators** to **ON** on the destination database before importing data.

Step 1 Log in to the FlexusX instance or device that can access the FlexusRDS instance.

Step 2 Connect to the FlexusRDS instance through a client.

Step 3 Import the table structure into the FlexusRDS instance.

```
# mysql -f -h<DB_ADDRESS>-P<DB_PORT>-uroot-p < <BACKUP_DIR>/dump-defs.sql
```

- *DB_ADDRESS* indicates the IP address of the FlexusRDS instance.

- *DB_PORT* indicates the DB instance port.
- *BACKUP_DIR* indicates the directory where **dump-defs.sql** is stored.

Example:

```
# mysql -f -h 172.16.66.198 -P 3306 -u root -p < dump-defs.sql
```

Enter password:

 NOTE

If you intend to import SQL statements of a table to FlexusRDS, specify a database in the command. Otherwise, the error message "No database selected" may be displayed. For example, if you intend to import SQL statements of a table to database **mydb**, run the following command:

```
# mysql -f -h 172.16.66.198 -P 3306 -u root -p mydb < dump-defs.sql
```

Enter password:

Step 4 Import data into the FlexusRDS instance.

```
# mysql -f -h<DB_ADDRESS>-P<DB_PORT>-uroot-p< <BACKUP_DIR>/dump-data.sql
```

- *DB_ADDRESS* indicates the IP address of the FlexusRDS instance.
- *DB_PORT* indicates the DB instance port.
- *BACKUP_DIR* indicates the directory where **dump-data.sql** is stored.

Example:

```
# mysql -f -h 172.16.66.198 -P 3306 -u root -p < dump-data.sql
```

Enter password:

 NOTE

If you intend to import SQL statements of a table to FlexusRDS, specify a database in the command. Otherwise, the error message "No database selected" may be displayed. For example, if you intend to import SQL statements of a table to database **mydb**, run the following command:

```
# mysql -f -h 172.16.66.198 -P 3306 -u root -p mydb < dump-defs.sql
```

Enter password:

Step 5 View the import result.

```
mysql> show databases;
```

The following result indicates that database **frdsdb** has been imported.

```
mysql> show databases;
+-----+
| Database          |
+-----+
| information_schema |
| frdsdb            |
| mysql             |
| performance_schema |
+-----+
4 rows in set (0.00 sec)
```

----End

3.3.2.2 Migrating Data to FlexusRDS Using the Export and Import Functions of DAS

Scenarios

Data Admin Service (DAS) is a one-stop management platform that allows you to manage Huawei Cloud databases on a web console. It offers database development, O&M, and intelligent diagnosis, making it easy to use and maintain databases.

To back up or migrate data, you can use DAS to export data from the source database first and then import the data to from your local PC or OBS bucket to the destination database.

For more information, see [Import and Export](#).

Constraints

- Only one file that is no larger than 1 GB can be imported at a time.
- Only data files in the CSV or SQL format can be imported.
- Binary fields such as BINARY, VARBINARY, TINYBLOB, BLOB, MEDIUMBLOB, and LONGBLOB are not supported.
- Data cannot be exported or imported using cross-region OBS buckets.

Exporting Data

Step 1 In the instance list, locate the target DB instance and click **Log In** in the **Operation** column.

Step 2 On the displayed login page, enter the username and password and click **Log In**.

Step 3 On the top menu bar, choose **Import and Export > Export**.

Step 4 On the displayed page, click **Create Task** and choose **Export Database** or **Export SQL Result** as required. The following takes database export as an example.

Alternatively, click **Quick Export** and select the target database. On the displayed page, select a storage path and click **OK**.

Figure 3-7 Quick export

Step 5 On the displayed page, set parameters as required in areas **Basic Information** and **Advanced Settings**. Then, select the tables to be exported on the right.

Figure 3-8 Creating an export task

Export Database
✕

Basic Information

Database: Export all tables

Allowed Rows:

File Type: SQL CSV

Object to Export: Data Structure Data and structure

Charset: UTF8 GBK

Storage: No OBS bucket? [Create OBS Bucket](#)
Creating an OBS bucket is free of charge, but storing files in it will incur fees.

Options: Combine INSERT statements. (Combine INSERT statements into files, with each file smaller than 5 MB.)
 Generate a file for each table. (Downloading table files in the details slows down the export.)

Remarks:

Advanced Settings ⌵

Tables

Selected Tables: 0

<input type="checkbox"/>	Table Name	Column	WHERE Clause
<input type="checkbox"/>	asd	Edit	Edit
<input type="checkbox"/>	dddd	Edit	Edit
<input type="checkbox"/>	new_db1_tb1	Edit	Edit
<input type="checkbox"/>	rule_aml_main	Edit	Edit
<input type="checkbox"/>	test1	Edit	Edit

10 / page Total Records: 5 < 1 >

NOTE

In a SQL result export task, the executed SQL statements cannot exceed 5 MB.

Export SQL Result
✕

Basic Information

Database:

Allowed Rows:

File Type: SQL-insert CSV

Charset: UTF8 GBK

Storage: No OBS bucket? [Create Bucket](#)
Creating an OBS bucket is free of charge, but storing files in it will incur fees.

Options: Combine INSERT statements. (Combine INSERT statements into files, with each file smaller than 5 MB.)
 Generate one file for each result.

SQL to Execute:

Remarks:

Advanced Settings ⌵

NOTE

- Databases are classified into user databases and system databases. System databases cannot be exported. If system database data is required, deploy system database services in a created user database, so that you can export the system database data from the user database.
- DAS connects to your standby database to export data. This prevents the primary database from being affected by data export. However, if the standby database has a high replication delay, the exported data may not be the latest.

Step 6 After settings are complete, click **OK**.

Step 7 In the task list, view the task ID, type, status, and progress.

Step 8 Click **Details** in the **Operation** column to view task details.

Figure 3-9 Task list

Task ID	Task Type	Database	Started	Ended	File Size	File Type	Status	Elapsed Time	Exported Rows	Progress	Remarks	Operation
c46815396084322816c539680992031	Quick E...	db_01	2020-09-07 20:16:45	2020-09-07 20:16:55	4.53 MB	SQL	Successful	10 secs...	202415	100%		Details Download
c2084378584741a0b437858a7e1a2	Database	create_new_db1	2020-09-03 16:50:45	2020-09-03 16:52:14	16.36 MB	SQL	Successful	1 min...	10000	100%		Details Download
7a959a295084689996c290d96f5ca	Database	create_new_db1	2020-09-03 16:47:05	2020-09-03 16:47:22	3.94 MB	SQL	Successful	17 secs...	2414	100%		Details Download

----End

Importing Data

Step 1 On the top menu bar, choose **Import and Export > Import**.

Step 2 Import a file from your local PC or an OBS bucket.

Figure 3-10 Creating an import task

Create Task

Import Type: **sql** | CSV

File Source: **Upload file** | Choose from OBS

Attachment Storage: 407154 | No OBS bucket? [Create OBS Bucket](#)

Creating an OBS bucket is free of charge, but storing files in it will incur fees.

Attachment:
 +
 Click here to upload a file, or drag one here. (.sql)
Upload only one attachment that is no larger than 1 GB.

Database: db_4eb3_0000

Charset: **Auto Detect** | UTF8 | GBK

Options:
 Ignore errors, that is, skip the step where the SQL statement fails to be executed.
 Delete the uploaded file upon an import success.

Remarks:
 [Text Area]

Create Cancel

- From your local PC
 In the upper left corner, click **Create Task**. On the displayed page, select an import type, select **Upload file** for **File Source**, set the attachment storage, and upload the file. Then, set other parameters as required.

For security purposes, imported files are stored in OBS buckets.

 **NOTE**

- To keep your data secure, provide your own OBS bucket to store the attachments you upload. In this way, DAS automatically connects to your OBS bucket for in-memory reading.
- If you select **Delete the uploaded file upon an import success.**, the file you uploaded will be automatically deleted from the OBS bucket after being imported to the destination database.
- From an OBS bucket
In the upper left corner, click **Create Task**. On the displayed page, select an import type, select **Choose from OBS** for **File Source**, and select a file from the bucket. Then, set other parameters as required.

 **NOTE**

The file uploaded from an OBS bucket will not be deleted upon an import success.

Step 3 After setting import parameters, click **Create**. Confirm the information again before you click **OK** because original data may be overwritten after data import.

Step 4 View the import progress in the task list or check task details.

----End

3.3.3 Permissions Management

3.3.3.1 Creating a User and Granting Permissions

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

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing FlexusRDS resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust a Huawei Cloud account or cloud service to perform efficient O&M on your FlexusRDS resources.

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

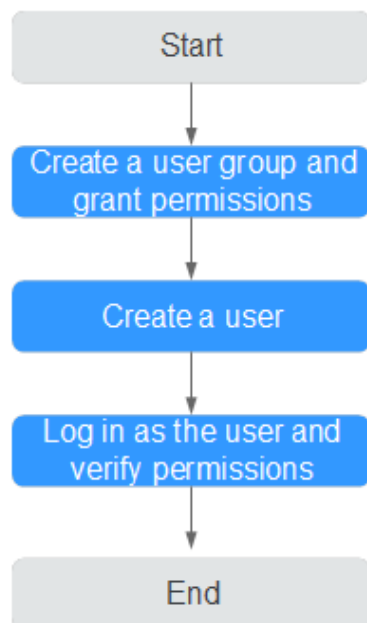
This section describes the procedure for granting permissions (see [Figure 3-11](#)).

Prerequisites

Learn about the permissions (see [Permissions](#)) supported by FlexusRDS and choose policies or roles according to your requirements. For the system policies of other services, see [System-defined Permissions](#).

Process Flow

Figure 3-11 Process for granting FlexusRDS permissions



1. **Create a user group and assign permissions** to it.

Create a user group on the IAM console, and attach the **RDS ReadOnlyAccess** policy to the group.

NOTE

To use some interconnected services, you also need to configure permissions of such services.

For example, to connect to your DB instance through the console, configure the **DAS FullAccess** permission of Data Admin Service (DAS) besides **RDS ReadOnlyAccess**.

1. **Create an IAM user and add it to the user group.**

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

2. **Log in** and verify permissions.

Log in to the console by using the created user, and verify that the user only has read permissions for FlexusRDS.

- Go to the FlexusRDS console and click **Buy FlexusRDS Instance** in the upper right corner. If a message appears indicating that you have insufficient permissions to perform the operation, the **RDS ReadOnlyAccess** policy has already been applied.
- Choose any other service. If a message appears indicating that you have insufficient permissions to access the service, the **RDS ReadOnlyAccess** policy has already taken effect.

3.3.3.2 FlexusRDS Custom Policies

Custom policies can be created to supplement the system policies of FlexusRDS.

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

- Visual editor: Select cloud services, actions, resources, and request conditions without the need to know policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see [Creating a Custom Policy](#). The following contains examples of common FlexusRDS custom policies.

Example Custom Policies

Example: Allowing users to create manual backups

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["rds:backup:create"]
  }]
}
```


3.3.4 Instance Modifications


3.3.4.1 Changing a DB Instance Name

Scenarios



You can change the name of a DB instance as required.

Procedure

Step 1 In the instance list, locate the instance that you want to edit name for and click  next to the instance name. Then, change the name and click **OK**.

Alternatively, click the target instance name. On the displayed page, click  under the **DB Instance Name** field and change the instance name.

The instance name must start with a letter and consist of 4 to 64 characters. Only letters (case-sensitive), digits, hyphens (-), underscores (_), and periods (.) are allowed.

- To submit the change, click .
- To cancel the change, click .

Step 2 Check the result in the instance list.

----End

3.3.4.2 Rebooting DB Instances

Scenarios

You may need to reboot a DB instance during maintenance. For example, after you modify some parameters, a reboot is required for the modifications to take effect. You can reboot one or more DB instances at a time on the console.

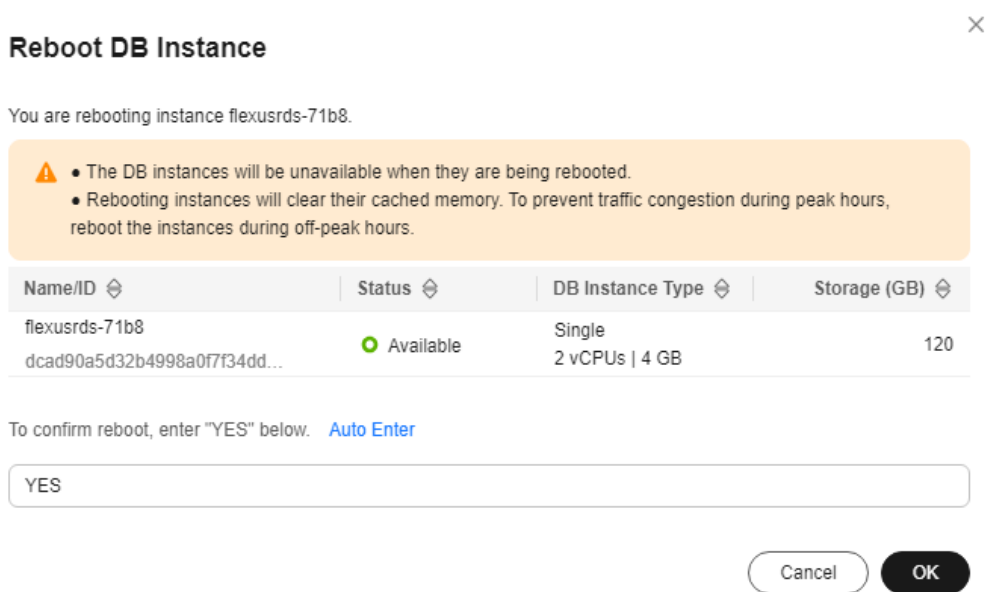
Constraints

- If the DB instance status is **Abnormal**, the reboot may fail.
- Rebooting a DB instance will reboot the DB engine service, causing service interruptions. During this period, the instance status is **Rebooting**.
- Rebooting DB instances will cause instance unavailability and clear cached memory. To prevent traffic congestion during peak hours, you are advised to reboot DB instances during off-peak hours.
- After a primary/standby DB instance is rebooted, it takes about one minute to establish the replication relationship. During this period, some operations, such as changing the instance class, cannot be performed.

Procedure

- Step 1** In the instance list, select one or more DB instances (maximum: 50) to be rebooted and click **Reboot** above the instance list.
- Step 2** In the displayed dialog box, enter **YES** and click **OK**.

Figure 3-12 Rebooting a DB instance



- Step 3** View the instance status. If the status is **Available**, the instance has been rebooted successfully.

----End

3.3.4.3 Resetting the Administrator Password

Scenarios

If you forget the password of the administrator account **root**, you can reset the password. The new password is applied immediately without rebooting the instance.

Precautions

- If the password you provide is regarded as a weak password by the system, you will be prompted to enter a stronger password.
- If you change the administrator password of a primary instance, the administrator password of the standby instance will also be changed.
- The time required for the new password to take effect depends on the amount of service data currently being processed by the primary DB instance.
- To protect against brute force hacking attempts and ensure system security, change your password periodically.

Procedure

- Step 1** In the instance list, locate the target instance and click **Reset Password** in the **Operation** column.
- Step 2** In the displayed dialog box, enter a new password and confirm the password.

Figure 3-13 Resetting the administrator password

Reset Password ×

DB instance ID: dcad90a5d32b4998a0f7f34dddafb954in01

DB Instance Name: flexusrds-71b8

New Password: 👁

Confirm Password: 👁

i After the password is reset, use the new password to access the DB instance.

Cancel OK

NOTICE

Keep this password secure. The system cannot retrieve it.

The password must consist of 8 to 32 characters and contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters (~ ! @ # \$ % ^ * - _ = + ? , () & . |). Enter a strong password and periodically change it for security reasons.

- To submit the new password, click **OK**.
- To cancel the reset operation, click **Cancel**.

----End

3.3.4.4 Storage Autoscaling

Scenarios

With storage autoscaling enabled, when FlexusRDS detects that you are running out of database space, it automatically scales up your storage.

Constraints

- If your account balance is insufficient, storage autoscaling will fail.
- The storage space can be autoscaled up only when your instance status is **Available** or **Storage full**.
- For a primary/standby DB instance, autoscaling the storage for the primary node will also autoscale the storage for the standby node.
- If a yearly/monthly DB instance has pending orders, it will not be autoscaled.

Procedure


- Step 1** In the instance list, click the target instance name.
- Step 2** On the **Overview** page, click **Configure** under the **Configure Autoscaling** field.
- Step 3** In the displayed dialog box, click  and configure the required parameters.

Figure 3-14 Configuring autoscaling

Configure Autoscaling

×

Enable Autoscaling

Additional storage will be billed. [Learn more](#) ↗

Trigger If Available Storage Drops To

10%
▾

If available storage drops to or below this value, your storage will autoscale.

Increment (%)

20

Enter an integer.

Autoscaling Limit (GB)

4000

Storage can autoscale to no more than 4000 GB.

i If your account balance is insufficient, autoscaling will fail.

Cancel

OK

Table 3-3 Parameter description

Parameter	Description
Enable Autoscaling	If you select this option, autoscaling is enabled.
Trigger If Available Storage Drops To	If the available storage drops to a specified threshold (10%, 15%, or 20%), autoscaling is triggered.
Increment (%)	Autoscaling increment, as a percentage. The default value range is from 5% to 50%.
Autoscaling Limit (GB)	The default value range is from 120 to 4,000. The limit must be no less than the storage of the DB instance.

Step 4 Click **OK**.

----End

3.3.4.5 Binding and Unbinding an EIP

Scenarios

You can bind an EIP to a DB instance for public accessibility, and you can unbind the EIP from the DB instance later if needed.

Precautions

- You can buy an EIP [on the network console](#) and bind it to a FlexusRDS instance. One EIP can be bound to only one instance. For pricing details, see [Elastic IP pricing details](#).
- If a DB instance has already been bound with an EIP, you must unbind the EIP from the instance first before binding a new EIP to it.

Binding an EIP to a DB instance

Step 1 In the instance list, click the target instance name.

Step 2 On the displayed **Overview** page, click **Bind** under the **EIP** field.

Step 3 In the displayed dialog box, all available EIPs are listed. Select the required EIP and click **Yes**.

Step 4 View the EIP that has been bound to the DB instance.

----End

Unbinding an EIP from a DB instance

Step 1 In the instance list, click the target instance name.

Step 2 On the displayed **Overview** page, click **Unbind** under the **EIP** field.

Step 3 In the displayed dialog box, click **Yes**.

----End

3.3.4.6 Renewing DB Instances

Scenarios

You can renew one or multiple yearly/monthly DB instances at a time.

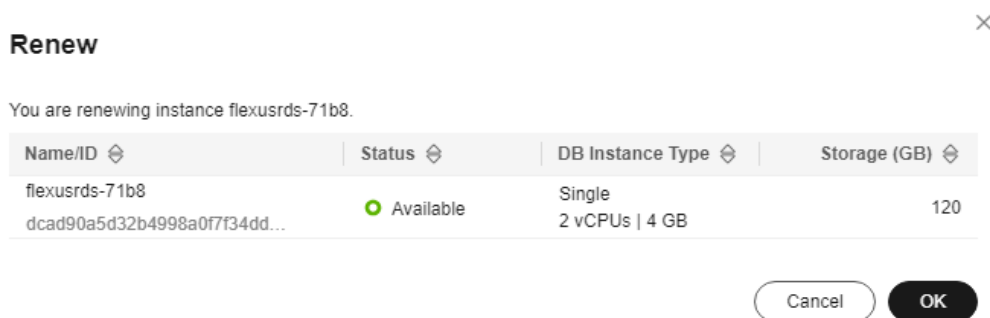
Procedure

Step 1 In the instance list, select the target DB instance and click **Renew** above the instance list.

You can also click the target instance name to go to the **Overview** page and renew the instance.

Step 2 In the displayed dialog box, confirm the instance to be renewed.

Figure 3-15 Renewing an instance



Step 3 Click **OK** to go to the renewal page and renew the instance.

----End

3.3.4.7 Unsubscribing a Yearly/Monthly DB Instance

Scenarios

To delete a DB instance billed on the yearly/monthly basis, you need to unsubscribe the order. For unsubscription fees, see [Unsubscription Rules](#).

Constraints

- A DB instance cannot be unsubscribed when any operations are being performed on it. It can be unsubscribed only after the operations are complete.
- If a backup of a DB instance is being restored, the instance cannot be unsubscribed.

Procedure

Step 1 In the instance list, select the target instance and click **Unsubscribe** above the instance list.

Step 2 In the displayed dialog box, enter **YES**.

Step 3 Click **OK**.

After you unsubscribe from an instance order, the instance will be deleted and it is no longer displayed in the instance list.

----End

3.3.5 Backups and Restorations

3.3.5.1 Creating a Manual Backup

Scenarios

FlexusRDS allows you to create manual backups for an available DB instance. You can use these backups to restore data.

Constraints

- You can create manual backups only when your account balance is no less than \$0 USD.
- Unsubscribing from a DB instance will delete its automated and manual backups.
- The system verifies the connection to the DB instance when starting a full backup task. If either of the following conditions is met, the verification fails and a retry is automatically performed. If the retry fails, the backup will fail.
 - DDL operations are being performed on the DB instance.
 - The backup lock failed to be obtained from the DB instance.

Billing

Backups are saved as packages in OBS buckets. For the billing details, see [How Is FlexusRDS Backup Data Billed?](#)

Procedure

- Step 1** In the instance list, click the target instance name.
- Step 2** Click **Backups & Restorations** and then click **Create Backup**.
- Step 3** In the displayed dialog box, enter a backup name and description, and click **OK**.

Figure 3-16 Creating a backup

Create Backup

×

i When the DB instance is being backed up, data is copied and then compressed and uploaded to OBS at an average speed of 300 MB/s. Creating a backup increases the disk I/O load. Perform this operation during off-peak hours.

DB instance ID dcad90a5d32b4998a0f7f34dddafb954in01

DB Instance Name flexusrds-71b8

* Backup Name ?

Description ?

0/256

Cancel
OK

- The backup name must consist of 4 to 64 characters and start with a letter. It can contain only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_).
- The description consists of a maximum of 256 characters and cannot contain carriage return characters or the following special characters: >!<"&'=
- The time required for creating a manual backup depends on the amount of data.

Step 4 View and manage the created backup on the **Backups & Restorations** page.

----End

3.3.5.2 Deleting a Manual Backup

Scenarios

You can delete manual backups to free up backup storage.

Constraints

- Deleted manual backups cannot be recovered.

- Manual backups that are being created cannot be deleted.

Procedure

Step 1 In the instance list, click the target instance name.

Step 2 Click **Backups and Restorations**.

Step 3 Locate a manual backup and click **Delete** in the **Operation** column.

The following backups cannot be deleted:

- Automated backups
- Backups that are being restored
- Backups that are being replicated

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

----End

3.3.5.3 Downloading a Full Backup

Scenarios

You can download manual and automated full backup files in .qp format for local storage.

Constraints

- Full backup files of frozen DB instances cannot be downloaded.
- When you use OBS Browser+ to download backup data, there is no charge for the outbound traffic from OBS.
- If the size of the backup data is greater than 400 MB, you are advised to use OBS Browser+ to download the backup data.

Method 1: Using OBS Browser+

Step 1 In the instance list, click the target instance name.

Step 2 Click **Backups and Restorations**.

Step 3 Locate the backup to be downloaded and click **Download** in the **Operation** column.

Step 4 In the displayed dialog box, select **Use OBS Browser+** for **Download Method** and click **OK**.

Figure 3-17 Using OBS Browser+

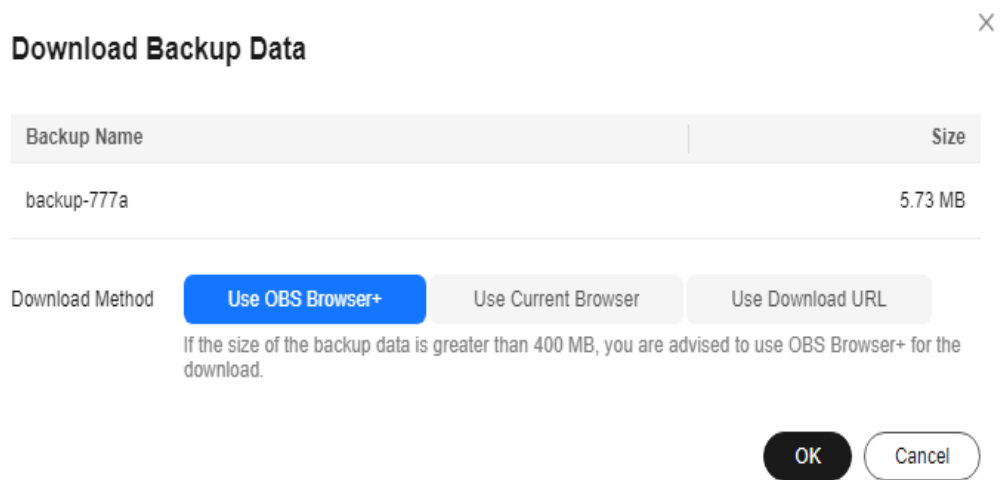
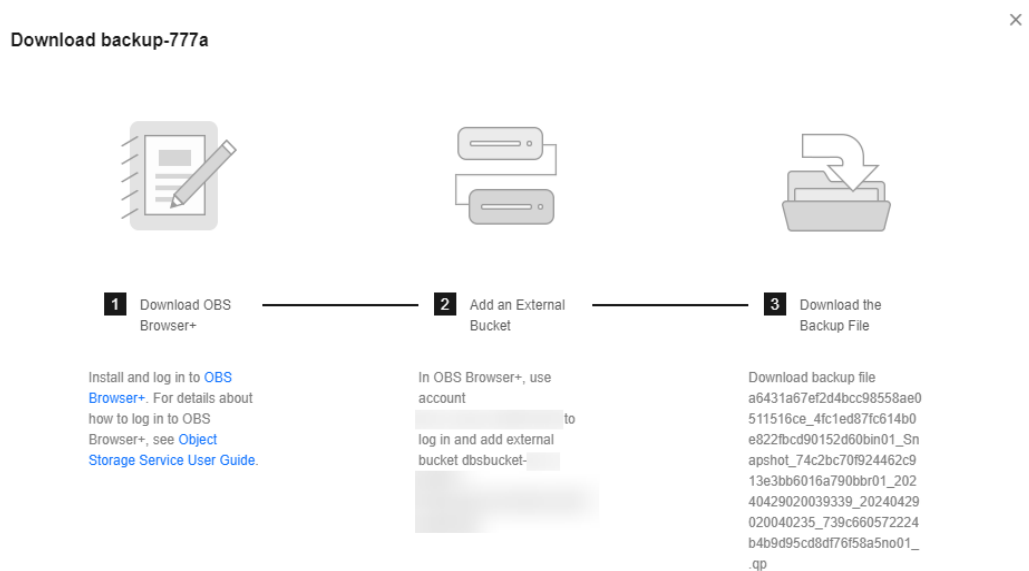
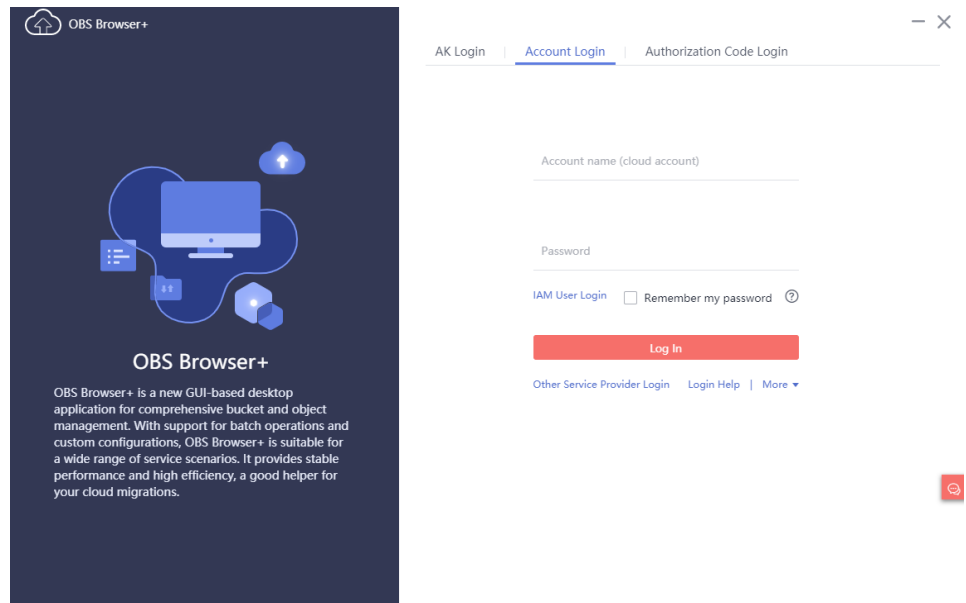


Figure 3-18 Download guide



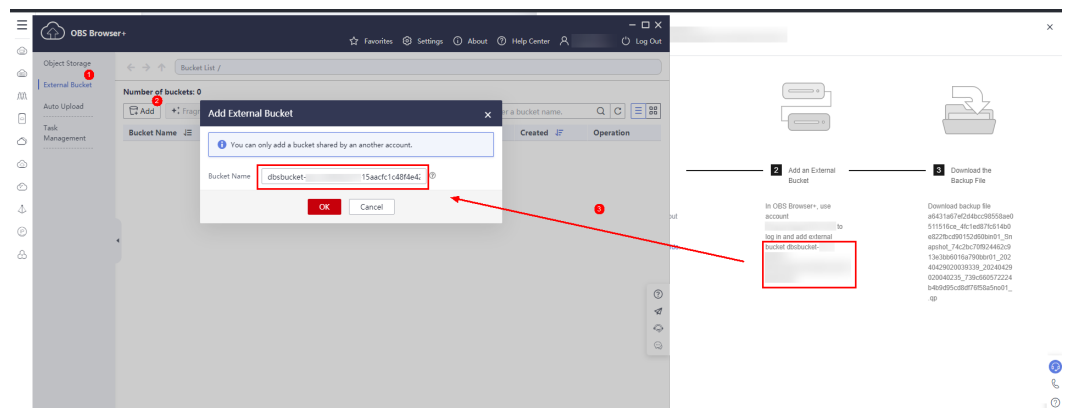
1. Download OBS Browser+ following step 1 provided on the download guide page.
2. Decompress and install OBS Browser+.
3. Log in to OBS Browser+ using the username provided in step 2 on the download guide page.

Figure 3-19 Logging in to OBS Browser+



4. Add an external bucket using the bucket name provided in step 2 on the download guide page.

Figure 3-20 Adding an external bucket



NOTE

If you want to access OBS external buckets across accounts, the access permission is required. For details, see [Granting IAM Users Under an Account the Access to a Bucket and the Resources in It](#).


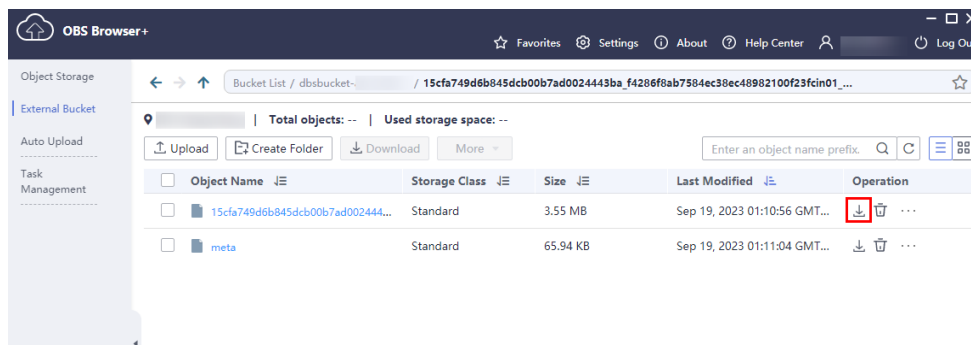
5. Download the backup file.
On the OBS Browser+ page, click the bucket that you added. In the search box on the right of the object list page, enter the backup file name provided in step 3 on the download guide page. In the search result, locate the target backup and click  in the **Operation** column.

Figure 3-21 Downloading a backup

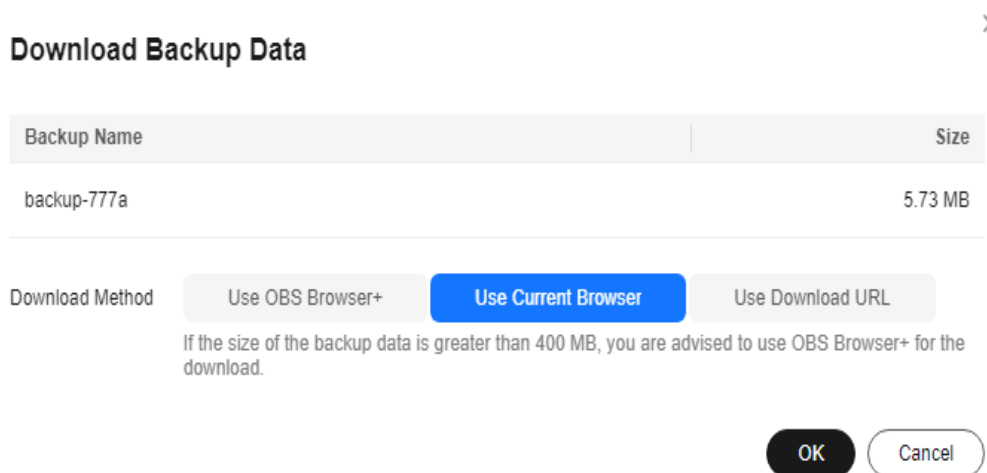


----End

Method 2: Using Current Browser

- Step 1** In the instance list, click the target instance name.
- Step 2** Click **Backups and Restorations**.
- Step 3** Locate the backup to be downloaded and click **Download** in the **Operation** column.
- Step 4** In the displayed dialog box, select **Use Current Browser** for **Download Method** and click **OK**.

Figure 3-22 Using the current browser



----End

Method 3: Using Download URL

- Step 1** In the instance list, click the target instance name.
- Step 2** Click **Backups and Restorations**.
- Step 3** Locate the backup to be downloaded and click **Download** in the **Operation** column.


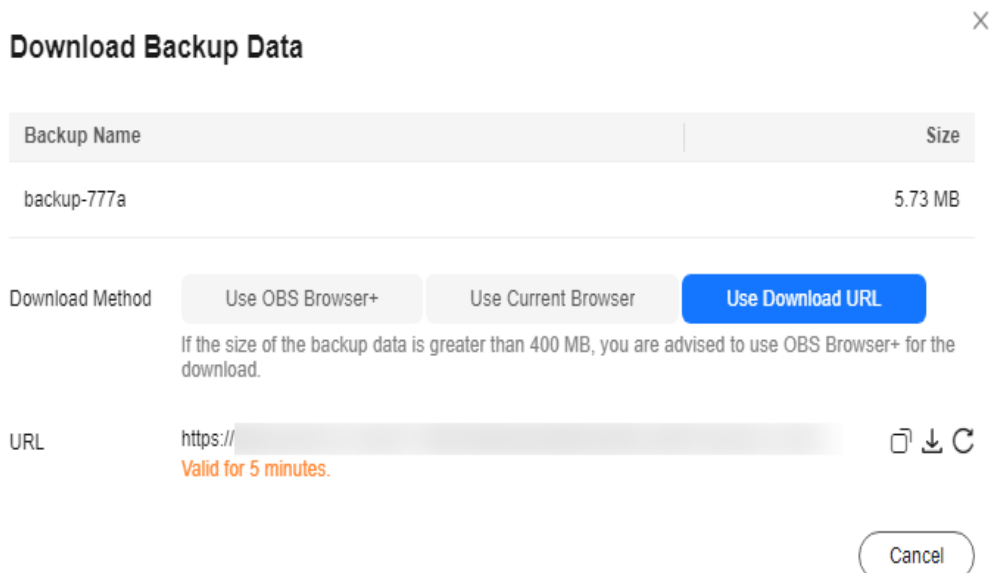
- Step 4** In the displayed dialog box, select **Use Download URL** for **Download Method**, click  to copy the URL, and enter the URL in your browser.

Figure 3-23 Using the download URL



- You can also run the following command to download backup files:
wget -O *FILE_NAME* --no-check-certificate "*DOWNLOAD_URL*"
The parameters in the command are as follows:
FILE_NAME: indicates the new backup file name after the download is successful. The original backup file name may be too long and exceed the maximum characters allowed by the client file system. You are advised to use the **-O** argument with wget to rename the backup file.
DOWNLOAD_URL: indicates the location of the backup file to be downloaded. If the location contains special characters, escape is required.

----End

3.3.5.4 Checking and Exporting Backup Information

Scenarios


You can export backup information of FlexusRDS instances to an Excel file for further analysis. The exported information includes the backup ID, backup name, backup type, backup method, backup start and end times, status, size, and description.

For details about how to export backup data, see [Downloading a Full Backup](#).

Procedure

- Step 1** In the instance list, click the target instance name.

Step 2 Click **Backups and Restorations**.

Step 3 Click  above the backup list to export backup information.

- If you want to export specified backup records, you can first select them and then export them. You can only select and export the backup records displayed on the current page.
- If you do not select any backup records, all backup records are exported by default. (A maximum of the first 5,000 backup records can be exported. If you want to export more, select the records and export them.)
- The backup information is exported to an Excel file for your further analysis.

Figure 3-24 Backup information

	A	B	C	D	E	F	G	H
1	Backup ID	Backup Name	Backup Type	Backup Method	Backup Time	Status	Size	Description
2	f08c648504944ba88ce2d143c27869d5br01	mysql-flexusrds-71b8	Automated	Physical backup	Jun 12, 2024 10:32:09	Completed	5.93 MB	--
3								

----End

3.3.5.5 Restoring a FlexusRDS Instance

3.3.5.5.1 Restoring an Instance from Backups

Scenarios

This section describes how to use an automated or manual backup to restore a DB instance to the status when the backup was created. The restoration is at the DB instance level.

When you restore a DB instance from a backup file, the backup file is downloaded from OBS and then restored to the DB instance at an average speed of 100 MB/s.

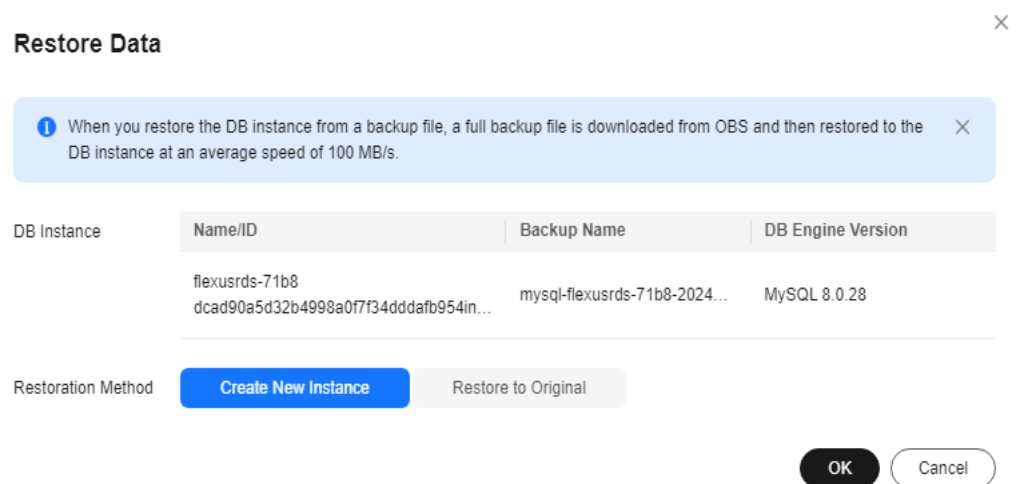
Constraints

- Constraints on restoring data to a new DB instance:
 - You can restore data to a new instance only when your account balance is greater than or equal to \$0 USD. You will pay for the new instance specifications.
 - The storage space of the new instance should be no less than that of the original instance.
 - If transparent page compression is enabled by specifying attributes in the CREATE TABLE statement for the original DB instance, the restoration may fail due to insufficient storage space.
- Constraints on restoring data to the original DB instance:
 - If the DB instance for which the backup is created has been deleted, data cannot be restored to the original DB instance.
 - Restoring to the original DB instance will overwrite all existing data and the DB instance will be unavailable during the restoration process.

Procedure

- Step 1** In the instance list, click the target instance name.
- Step 2** Click **Backups and Restorations**.
- Step 3** Locate the backup to be restored and click **Restore** in the **Operation** column.
- Step 4** Select a restoration method and click **OK**.
 - Create New Instance

Figure 3-25 Restoring data to a new instance



The **Create New Instance** page is displayed.

- The DB engine version of the new instance is the same as that of the original instance.
- The storage space of the new instance must be no less than that of the original instance.
- Restore to Original

Figure 3-26 Restoring data to the original instance

Restore Data

When you restore the DB instance from a backup file, a full backup file is downloaded from OBS and then restored to the DB instance at an average speed of 100 MB/s.

DB Instance	Name/ID	Backup Name	DB Engine Version
	flexusrds-71b8 dcad90a5d32b4998a0f7f34dddafb954in...	mysql-flexusrds-71b8-2024...	MySQL 8.0.28

Restoration Method:

I acknowledge that after I select Restore to Original, data on the original databases will be overwritten and the original DB instance will be unavailable during the restoration.

- Select **I acknowledge that after I select Restore to Original, data on the original databases will be overwritten and the original DB instance will be unavailable during the restoration.** and click **Next**.
- Confirm the information and click **OK**.

Step 5 View the restoration result. The result depends on which restoration method was selected:

- Create New Instance

A new DB instance is created using the backup data. The instance status changes from **Creating** to **Available**.

The new DB instance is independent from the original one. After the new instance is created, a full backup will be automatically triggered.

- Restore to Original

In the instance list, the status of the original DB instance changes from **Restoring** to **Available**. After the restoration is complete, a full backup will be automatically triggered.

----End

3.3.5.5.2 Restoring an Instance to a Point in Time

Scenarios

You can use automated backups to restore an instance to a specific point in time.

When you enter the time point that you want to restore the DB instance to, FlexusRDS downloads the most recent full backup file from OBS to the DB instance. Then, incremental backups are also restored to the specified point in time on the DB instance. Data is restored at an average speed of 100 MB/s.

Constraints

- Do not run the **reset master** command on instances within their lifecycle. Otherwise, an exception may occur during the point-in-time recovery (PITR).
- Constraints on restoring data to a new DB instance:
 - You can restore data to a new instance only when your account balance is greater than or equal to \$0 USD. You will pay for the new instance specifications.
 - The storage space of the new instance should be no less than that of the original instance.
 - When you restore data to a new DB instance, large transactions in the original DB instance backup may cause a restoration failure. If the restoration fails, contact customer service.
- Constraints on restoring data to the original DB instance:
 - Restoring to the original DB instance will overwrite data on it and cause the DB instance to be unavailable during the restoration.

Procedure

Step 1 In the instance list, click the target instance name.

Step 2 Click **Backups and Restorations**.

Step 3 Click **Restore** above the backup list.

Step 4 Select the restoration date and time range, enter a time point within the selected time range, and select a restoration method. Then, click **OK**.

- Create New Instance

Figure 3-27 Restoring data to a new instance

Restore Data ×

! When you restore the DB instance from a backup file, a full backup file is downloaded from OBS and then restored to the DB instance at an average speed of 100 MB/s. ×

Restore To: ⌵

Time Range: ⌵

Time Point: ⌵

Restoration Method: **Create New Instance** Restore to Original

The **Create New Instance** page is displayed.

- The DB engine and version of the new DB instance are the same as those of the original DB instance and cannot be changed.

- The storage space of the new instance should be no less than that of the original instance.
- Restore to Original

Figure 3-28 Restoring data to the original instance

Restore Data ×

i When you restore the DB instance from a backup file, a full backup file is downloaded from OBS and then restored to the DB instance at an average speed of 100 MB/s. ×

Restore To: Apr 28, 2024 📅

Time Range: Apr 28, 2024 00:00:00 – Apr 28, 2024 21:01:48 GMT+08:00 ▼

Time Point: 21:01:48 🕒

Restoration Method: Create New Instance Restore to Original

I acknowledge that after I select Restore to Original, data on the original databases will be overwritten and the original DB instance will be unavailable during the restoration.

Next Cancel

- Select **I acknowledge that after I select Restore to Original, data on the original databases will be overwritten and the original DB instance will be unavailable during the restoration.** and click **Next**.
- Confirm the information and click **OK**.

Step 5 View the restoration result. The result depends on which restoration method was selected:

- **Create New Instance**
A new DB instance is created using the backup data. The instance status changes from **Creating** to **Available**.
The new DB instance is independent from the original one. After the new DB instance is created, a full backup will be automatically triggered.
- **Restore to Original**
In the instance list, the status of the DB instance changes from **Restoring** to **Available**.
A new restoration time range is available. There will be a difference between the new and original time ranges. This difference reflects the duration of the restoration.
After the restoration is complete, a full backup will be automatically triggered.

----End

3.3.6 Parameters

3.3.6.1 Suggestions on Parameter Tuning

Parameters are key configuration items in a database system. Improper parameter settings may adversely affect database performance. This section describes some important parameters for your reference. For details, visit the [MySQL official website](#).

For details on how to modify FlexusRDS parameters on the console, see [Modifying Instance Parameters](#).

Sensitive Parameters

- **innodb_flush_log_at_trx_commit**

Default value: **1**

Function: Controls the balance between strict ACID compliance for commit operations and higher performance. The default setting of **1** is required for full ACID compliance. Logs are written and flushed to disks at each transaction commit. If the value is set to **0**, logs are written and flushed to disks once per second. If the value is set to **2**, logs are written at each transaction commit and flushed to disks every two seconds.

Impact: If this parameter is not set to **1**, data security is not guaranteed. If the system fails, data may be lost.

Recommended value for POC: **2**

- **sync_binlog**

Default value: **1**

Function: Controls how often the MySQL server synchronizes binary logs to the disk. The default setting of **1** requires synchronization of the binary log to the disk at each transaction commit. If the value is set to **0**, synchronization of the binary log to the disk is not controlled by the MySQL server but relies on the OS to flush the binary log to the disk. This setting provides the best performance. However, if a power failure occurs or the OS crashes, all binary log information in **binlog_cache** will be lost.

Impact: If this parameter is not set to **1**, data security is not guaranteed. If the system fails, binary logs may be lost.

Recommended value for POC: **1000**

- **innodb_buffer_pool_size**

Default value: Varies depending on the DB instance classes.

Function: Specifies the size of the InnoDB buffer pool. The InnoDB buffer pool is used to cache table and index data. Increasing the value of this parameter reduces disk I/O.

Impact: Setting this parameter to a large value may cause system breakdown. Exercise caution when changing this parameter value.

Recommended value for POC: 70% to 75% of the memory for your DB instances with 32 GB memory or above

Performance Parameters

- The values of **innodb_spin_wait_delay** and **query_alloc_block_size** are determined by the DB instance specifications. If you increase their values, database performance may be affected.

- **max_connections**: indicates the total number of clients that can be concurrently connected. The default value of this parameter depends on the system architecture. System built-in connections occupy some connections specified by this parameter. To prevent concurrent connection conflicts, you are advised not to set this parameter to a value less than 30. This parameter cannot be set to a value smaller than the number of current connections.
- The default values of the following parameters are determined by the DB instance specifications: **innodb_buffer_pool_size**, **max_connections**, and **back_log**. These parameter values are **default** before being specified.
- The values of **innodb_io_capacity_max** and **innodb_io_capacity** are determined by the storage type. These parameter values are **default** before being specified.

Associated Parameters

- **character_set_server**: If you change the value of this parameter, the system changes the value of **collation_server** accordingly.
The parameters **character_set_server** and **collation_server** are correlated with each other. For example, for MySQL 5.7, when **character_set_server** is **latin1**, the default value of **collation_server** is **latin1_swedish_ci**. The **collation_server** value must start with **latin1**.
- **innodb_io_capacity**: The value of this parameter must be less than or equal to the value of **innodb_io_capacity_max**. For example, if **innodb_io_capacity_max** is set to **2000**, the maximum value of **innodb_io_capacity** is **2000**.

Constraints on Parameter Modification

- When the **innodb_adaptive_hash_index** and **innodb_buffer_pool_size** parameters are modified at the same time, the value of **innodb_adaptive_hash_index** will fail to be changed from **OFF** to **ON**.
- If **innodb_buffer_pool_instances** is set to **2**, the value of **innodb_buffer_pool_size** must be greater than or equal to 1 (unit: GB).

Other Parameters

- **max_prepared_stmt_count**: limits the upper limit of prepared statements. Too many prepared statements consume server memory resources. If this parameter is set to a small value, your DB instance may be vulnerable to the denial of service (DoS) attacks. You are advised to change this parameter value based on service requirements.
- The values of the following parameters will be adjusted based on kernel rules:
 - **key_cache_age_threshold**: automatically adjusted to a multiple of 100.
 - **join_buffer_size** and **key_cache_block_size**: automatically adjusted to multiples of 128.
 - **query_prealloc_size**, **innodb_log_buffer_size**, **max_allowed_packet**, and **thread_stack**: automatically adjusted to multiples of 1024.
 - **read_buffer_size**, **read_rnd_buffer_size**, **binlog_cache_size**, and **binlog_stmt_cache_size**: automatically adjusted to multiples of 4096.
- **innodb_strict_mode**: restricts the InnoDB check policy. The default value is **OFF**.

- **binlog_rows_query_log_events**: controls whether to write original SQL statements into binlogs. If this parameter is set to **ON**, database performance may deteriorate when a large amount of data is updated. Before you change the parameter value, consider the compatibility with tools such as Otter.

3.3.6.2 Modifying Instance Parameters

Scenarios

You can change parameter values in a custom parameter template and apply it to optimize FlexusRDS database performance.

Modifying a Single Parameter

- Step 1** In the instance list, click the target instance name.
- Step 2** Click the **Parameters** tab.
- Step 3** In the parameter list, locate the parameter you want to modify and click **Modify** in the **Operation** column.

NOTICE

After you modify a parameter, check the value in the **Effective upon Reboot** column.

- If the value is **Yes** and the instance status in the instance list is **Parameter change. Pending reboot**, a reboot is required for the modifications to take effect.

If you have modified parameters of a primary DB instance, you need to reboot the primary DB instance for the modifications to take effect. (For primary/standby DB instances, the parameter modifications are also applied to the standby DB instance.)

- If the value is **No**, the modifications take effect immediately.

Figure 3-29 Parameters

Parameter Name	Effective upon Reboot	Value	Allowed Values	Description	Operation
auto_increment_increment	No	1	1-65,535	auto_increment_increment and auto_increment_offset control operations in the AUTO_INCREMENT.	Modify
auto_increment_offset	No	1	1-65,535	auto_increment_increment and auto_increment_offset control operations in the AUTO_INCREMENT.	Modify
back_log	Yes	1000	1-65,535	Number of valid connection requests that MySQL can have. This comes into play when the...	Modify
binlog_cache_size	No	32768	4,096-16,777,216	The cache capacity used to store SQL statements for the binary log in a transaction.	Modify
binlog_checksum	No	CRC32	NONE,CRC32	When this variable is enabled, the primary server writes a checksum for each event in the...	Modify
binlog_rows_query_log_events	No	OFF	ON,OFF	Once the parameter is enabled, a MySQL 5.6.2 or later server writes information to log ev...	Modify
binlog_stmt_cache_size	No	32768	4,096-16,777,216	This variable determines the size of the cache for the binary log to hold non-transactional...	Modify
block_encryption_mode	No	aes-128-ecb	aes-128-ecb,aes-192-ecb,aes-256-ecb,aes-...	Controls the block encryption mode for block-based algorithms such as AES. It affects enc...	Modify
bulk_insert_buffer_size	No	8388608	0-18,446,744,073,709,551,615	Limits the size of the MyISAM cache tree in bytes per thread.	Modify
character_set_server	Yes	utf8mb4	utf8latin1gb,utf8mb4	The server's default character set.	Modify

- To save the modifications, click **Confirm**. In the displayed dialog box, click **Yes**.

- To cancel the modifications, click **Cancel**.


To view the change history, click **Change History** above the parameter list. The change history of the last seven days is displayed.

----End

Modifying Parameters in Batches

Step 1 In the instance list, click the target instance name.

Step 2 Click the **Parameters** tab.

Step 3 Switch on the batch modification switch . A maximum of 30 parameters can be modified at a time.

NOTICE

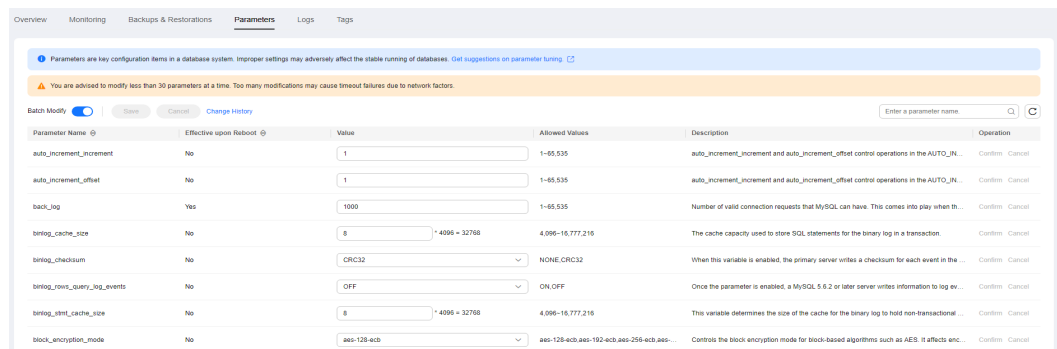
After you modify a parameter, check the value in the **Effective upon Reboot** column.

- If the value is **Yes** and the instance status in the instance list is **Parameter change. Pending reboot**, a reboot is required for the modifications to take effect.

If you have modified parameters of a primary DB instance, you need to reboot the primary DB instance for the modifications to take effect. (For primary/standby DB instances, the parameter modifications are also applied to the standby DB instance.)

- If the value is **No**, the modifications take effect immediately.

Figure 3-30 Modifying parameters



- To save your modifications, click **Save**. In the displayed dialog box, click **Yes**.
- To cancel your modifications, click **Cancel**. In the displayed dialog box, click **Yes**.

To view the change history, click **Change History** above the parameter list. The change history of the last seven days is displayed.

----End

3.3.6.3 Export a Parameter List

Scenarios

You can also export the parameter information (including parameter names, values, and descriptions) of a DB instance to a CSV file for viewing and analyzing details.

Procedure

- Step 1** In the instance list, click the target instance name.
- Step 2** Click the **Parameters** tab.
- Step 3** Click **Export** above the parameter list.

Figure 3-31 Export a parameter list



- Step 4** In the displayed dialog box, enter a file name and click **OK**.

NOTE

The file name can contain 4 to 81 characters.

----End

3.3.7 Logs

3.3.7.1 Viewing and Downloading Error Logs

FlexusRDS log management allows you to view database-level logs, including error logs and slow SQL query logs.

Error logs help you analyze problems with databases. You can download error logs for further analysis.

You can view error logs generated within the last month.

Viewing Log Details


Step 1 In the instance list, click the target instance name.

Step 2 Click the **Logs** tab. On the **Error Logs** tab page, view details about error logs.

- You can select a log level in the upper right corner to view logs of the selected level.

NOTE

For FlexusRDS instances, the following levels of logs are displayed:

- All log levels
- ERROR
- WARNING
- NOTE
- Error logs are displayed in log loading mode. There is no upper limit on the number of log records displayed within the query time range, and the total number of log records is not displayed.
- You can click  in the upper right corner to view logs generated in different time segments.
- If the description of a log is truncated, locate the log and move your pointer over the description in the **Description** column to view details.

----End

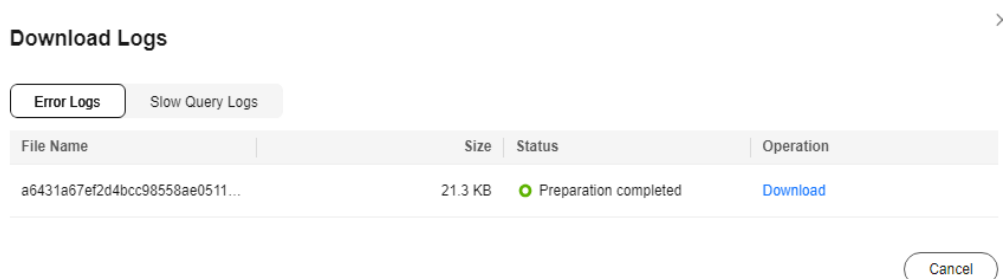
Downloading an Error Log

Step 1 In the instance list, click the target instance name.

Step 2 Click the **Logs** tab and click **Download Logs** on the right.

Step 3 Locate the log file whose status is **Preparation completed** and click **Download** in the **Operation** column.

Figure 3-32 Downloading an Error Log



- The system automatically loads the downloading preparation tasks. The loading duration is determined by the log file size and network environment.
 - When the log is being prepared for download, the log status is **Preparing**.
 - When the log is ready for download, the log status is **Preparation completed**.

- If the preparation for download fails, the log status is **Abnormal**.

Logs in the **Preparing** or **Abnormal** status cannot be downloaded.

- If the size of a log to be downloaded is greater than 40 MB, you need to use OBS Browser+ to download it. For details, see [Method 1: Using OBS Browser+](#).
- The download link is valid for 5 minutes. After the download link expires, a message is displayed indicating that the download link has expired. If you need to redownload the log, click **OK**.
- The downloaded logs contain only the logs of the primary node.

----End

3.3.7.2 Viewing and Downloading Slow Query Logs

Scenarios

Slow query logs record statements that exceed the **long_query_time** value (1 second by default). You can view log details and statistics to identify statements that are executing slowly and optimize the statements. You can also download slow query logs for service analysis.

Slow query logs generated within the last 7 days can be viewed.

FlexusRDS supports the following statement types:

- All statement types
- SELECT
- INSERT
- UPDATE
- DELETE
- CREATE

Parameter Description

Table 3-4 Parameters related to slow queries

Parameter	Description
long_query_time	Specifies how many microseconds a SQL query has to take to be defined as a slow query log. The default value is 1s. When the execution time of an SQL statement exceeds the value of this parameter, the SQL statement is recorded in slow query logs. The recommended value is 1s . Note: The lock wait time is not calculated into the query time.
log_queries_not_using_indexes	Specifies whether to record the slow query without indexes. The default value is OFF .

Parameter	Description
log_throttle_queries_not_using_indexes	Limits the number of SQL statements without indexes per minute that can be written to the slow query log. The default value is 0 .

Viewing Log Details

Step 1 In the instance list, click the target instance name.

Step 2 Click the **Logs** tab. On the **Slow Query Logs** tab page, view details about slow SQL statements.

NOTE

- You can view the slow query log records of a specified execution statement type or a specific time period.
- Only SELECT statements return the number of result rows. The number of result rows for the INSERT, UPDATE, DELETE, and CREATE statements is 0 by default.
- You can view slow query logs of a specified database name (which cannot contain any special characters). The database name supports only exact search.
- Slow query logs only record executed statements whose execution duration exceeds the threshold.
- The **long_query_time** parameter determines when a slow query log is recorded. However, changes to this parameter do not affect already recorded logs. If **long_query_time** is changed from 1s to 0.1s, FlexusRDS starts recording statements that meet the new threshold and still displays the previously recorded logs that do not meet the new threshold. For example, a 1.5s SQL statement that was recorded when the threshold was 1s will not be deleted now that the new threshold is 2s.
- Slow query logs are displayed in log loading mode. There is no upper limit on the number of log records displayed within the query time range, and the total number of log records is not displayed.
- If the length of a single line of an SQL statement exceeds 10 KB or the total number of lines exceeds 200, the SQL statement will be truncated. When you view slow query log details, the SQL statement may be incomplete after special processing and is for reference only.

----End

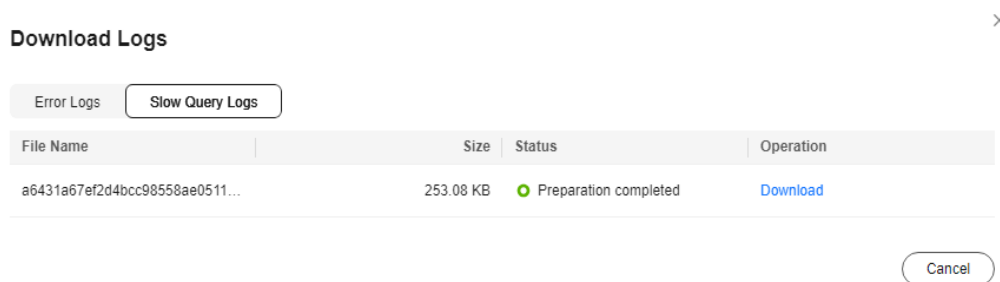
Downloading a Slow Query Log

Step 1 In the instance list, click the target instance name.

Step 2 Click the **Logs** tab and click **Download Logs** on the right.

Step 3 In the displayed dialog box, click **Slow Query Logs**.

Step 4 Locate the log file whose status is **Preparation completed** and click **Download** in the **Operation** column.

Figure 3-33 Downloading a Slow Query Log

- The system automatically loads the downloading preparation tasks. The loading duration is determined by the log file size and network environment.
 - When the log is being prepared for download, the log status is **Preparing**.
 - When the log is ready for download, the log status is **Preparation completed**.
 - If the preparation for download fails, the log status is **Abnormal**. Logs in the **Preparing** or **Abnormal** status cannot be downloaded.
- Only logs no more than 40 MB can be downloaded directly from this page. The time range is calculated from the time you download the logs back to the time when the accumulated file size reaches 40 MB.
- It is impossible to generate a log file much larger than 40 MB, like 100 MB or 200 MB. If a log file that is a little larger than 40 MB is required, use OBS Browser+ to download it by referring to [Method 1: Using OBS Browser+](#).
- The download link is valid for 5 minutes. After the download link expires, a message is displayed indicating that the download link has expired. If you need to redownload the log, click **OK**.
- The downloaded logs contain only the logs of the primary node.

----End

3.3.8 Interconnection with CTS

3.3.8.1 Key Operations Supported by CTS

With Cloud Trace Service (CTS), you can record operations associated with FlexusRDS instances for later query, audit, and backtrack operations.

Table 3-5 FlexusRDS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a DB instance or restoring data to a new instance	instance	createInstance
Enabling autoscaling	instance	instanceAction
Rebooting a DB instance	instance	instanceRestart

Operation	Resource Type	Trace Name
Restoring data to the original DB instance	instance	instanceRestore
Renaming a DB instance	instance	instanceRename
Resetting a password	instance	resetPassword
Setting database version parameters	instance	setDBParameters
Binding or unbinding an EIP	instance	setOrResetPublicIP
Adding a tag	instance	createTag
Deleting a tag	instance	deleteTag
Editing a tag	instance	modifyTag
Deleting a DB instance	instance	deleteInstance
Creating a backup	backup	createManualSnapshot
Downloading a backup (using OBS)	backup	downloadSnapshot
Downloading a backup (using a browser)	backup	backupsDownload
Deleting a backup	backup	deleteManualSnapshot
Deleting a frozen DB instance	all	rdsUnsubscribeInstance
Freezing a DB instance	all	rdsfreezeInstance
Renewing a DB instance	all	bssUpdateMetadata

3.3.8.2 Viewing Traces

For details about how to view audit logs, see [Querying Real-Time Traces](#).

3.3.9 Managing Tags

Scenarios

Tag Management Service (TMS) enables you to use tags on the management console to manage resources. TMS works with other cloud services to manage tags. TMS manages tags globally. Other cloud services manage only their own tags.

- Log in to the management console and choose **Management & Governance > Tag Management Service**. Set predefined tags on the TMS console.

- A tag consists of a key and value. You can add only one value for each key.
- Each DB instance can have up to 20 tags.

Editing a Tag

Step 1 In the instance list, click the target instance name.

Step 2 Click the **Tags** tab and click **Edit Tag**.

Step 3 In the displayed dialog box on the right, click **Add Tag**, enter a tag key and value, and click **OK**.

- The tag key must be unique. It must consist of 1 to 128 characters and can include letters, digits, spaces, and the following characters: `_ . : = + - @`. It cannot start or end with a space, or start with `_sys_`.
- The tag value (optional) can consist of up to 255 characters and can include letters, digits, spaces, and the following characters: `_ . : / = + - @`.

Step 4 After a tag has been added, you can view and manage it on the **Tags** page.

----End

Deleting a Tag

Step 1 In the instance list, click the target instance name.

Step 2 Click the **Tags** tab and click **Edit Tag**.

Step 3 In the displayed dialog box on the right, select the tag to be deleted and click **Delete**.

Step 4 Click **OK**.

After a tag has been deleted, it will no longer be displayed on the **Tags** page.

----End

3.3.10 Managing Quotas

What Is a Quota?

A quota is a limit on the quantity or capacity of a certain type of service resources available to you. Examples of FlexusRDS quotas include the maximum number of DB instances that you can create. Quotas are put in place to prevent excessive resource usage.

If a quota cannot meet your needs, apply for a higher quota.

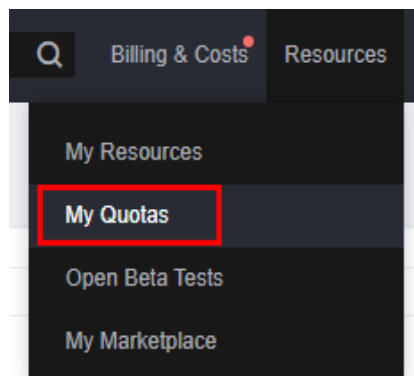
Viewing Quotas

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

Step 2 Click  in the upper left corner and select a region and project.

Step 3 In the upper right corner of the page, choose **Resources > My Quotas**.

Figure 3-34 My quotas



Step 4 On the **Quotas** page, view the used and total quotas of each type of resources.

----End

Increasing Quotas

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

Step 2 Click  in the upper left corner and select a region and project.

Step 3 In the upper right corner of the page, choose **Resources > My Quotas**.

Step 4 In the upper right corner of the page, click **Increase Quota**.

Figure 3-35 Increasing quotas

Service Quota			Increase Quota
Service	Resource Type	Used Quota	Total Quota
Auto Scaling	AS group	0	
Image Management Service	AS configuration	0	
Cloud Container Engine	Image	0	
	Cluster	0	
FunctionGraph	Function	0	
	Code storage(MB)	0	
	Event	3	
Elastic Visualize Service	Event (capacity/CPU)	120	
	Resource	4	
Storage Disaster Recovery Service	Protection group	0	
	Protection plan	0	
Cloud Backup Service	Backup Capacity(CB)	0	
	Backup	0	
Scalable File Service	File system	0	
	File system Capacity(CB)	0	
	Quota name	0	
	File URL, refresh	0	
CDN	Directory URL, refresh	0	
	URL, refresh	0	

Step 5 On the **Create Service Ticket** page, configure parameters as required.

In the **Problem Description** area, enter the required quota and reason for the quota adjustment.

Step 6 After all required parameters are configured, select the agreement and click **Submit**.

----End

4 Change History

Released On	Description
2024-05-30	This issue is the fourth official release. Added the following content: <ul style="list-style-type: none">• Overview• Logging In to a FlexusL Instance Linux Server (Using CloudShell)• Batch Reinstalling OSs
2024-05-15	This issue is the third official release. Added the FlexusX user guide.
2024-04-30	This issue is the second official release. Added the FlexusRDS user guide.
2024-04-15	The issue is the first official release.