Flexus L Instance

User Guide

Issue	01
Date	2024-09-25

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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 Purchasing a FlexusL Instance

Scenarios

This section describes how to purchase a FlexusL instance.

You can configure the region, image, instance specifications, required duration, and other parameters for your FlexusL instances based on your service requirements.

Constraints

If you want to create a FlexusL instance from a private image, learn about the restrictions on using private images.

Table 1-1 Restrictions on private images of FlexusL instances

Item	Description
Region	The FlexusL instance and private image must be in the same region, or no private image is available for the FlexusL instance. Therefore, before creating a FlexusL instance from a private image, create a private image in the region where the target FlexusL instance resides.
Server architecture	Only x86 is supported.

Item	Description
Image type	Only system disk private images are supported. Data disk private images and full-server private images are not supported. • Linux system disk images only support the following image sources: free public Linux images provided by Huawei Cloud, images created from FlexusL instances that are created using application images, and third-party private images you have imported. Other billed Linux images created from KooGallery images are not supported. • Windows system disk images with the Bring Your Own License (BYOL) license are supported. **NOTE** FlexusL instances do not support full-server images. If you want to migrate an entire server to a FlexusL instance, use Server Migration Service (SMS). For details, see **Migrating Servers Using Server Migration Service (SMS)**.
Password reset plug-in	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?**

Preparations

1. Before purchasing a FlexusL instance, sign up for a HUAWEI ID and enable Huawei Cloud services. For details, see **Signing Up a HUAWEI ID and Enabling Huawei Cloud Services** and **Completing Real-Name Authentication**.

   If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.
2. Ensure that your account has sufficient balance. If not, **top up your account**.

3. Before using a private image to create a FlexusL instance, use **Image Management Service (IMS)** to create an image first.

CAUTION

Before creating images, make sure you have learned about the **restrictions on private images of FlexusL instances**.

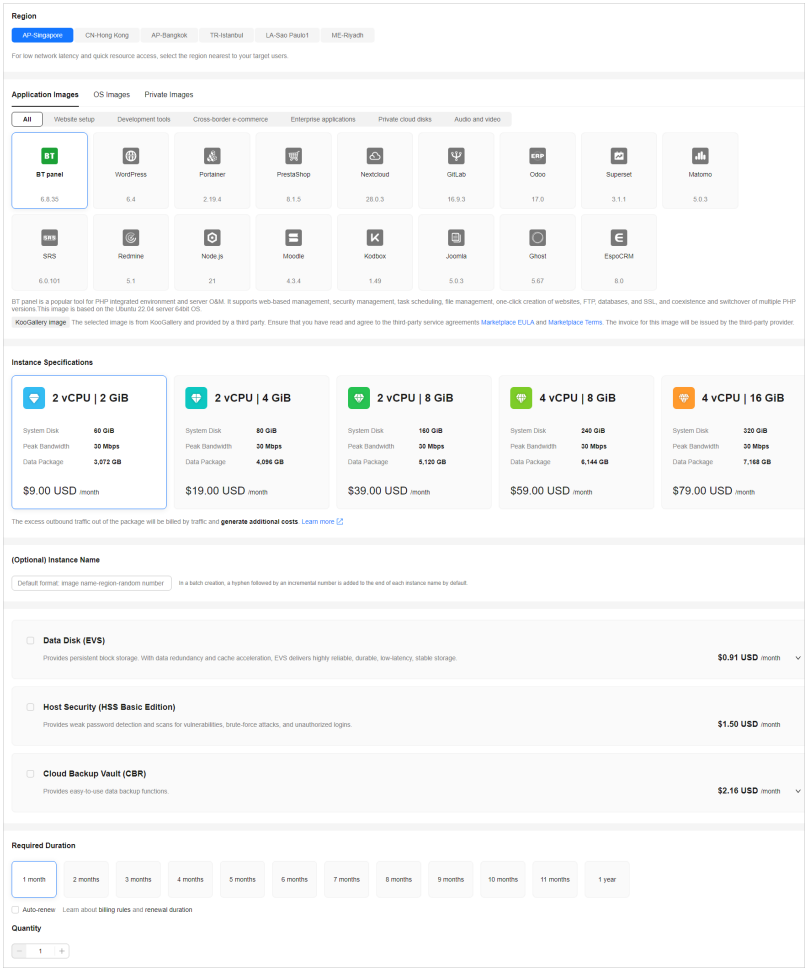
Table 1-2 Creating an image using IMS

Scenario	Description	Related Operations
Scenario 1	If your private image is created from a FlexusL instance, FlexusX instance, or ECS, it can be used in the current region. If you want to use the private image in another region, replicate the image to the region where you want to use it first.	• **Creating a System Disk Image from a Windows ECS** • **Creating a System Disk Image from a Linux ECS** • **Replicating Images Across Regions**
Scenario 2	If your private image is created on another cloud platform or downloaded from a third party, import the private image using IMS. Refer to the operation guide based on the image file format: • External image files can be in any of the following formats: VMDK, VHD, QCOW2, RAW, VHDX, QED, VDI, QCOW, ZVHD2, and ZVHD. • ISO files.	• **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	If you want to use a private image of another Huawei account, ask the account owner to share the image with you and replicate the shared image as a private image.	• **Sharing Images** • **Replicating a Shared Image**

Procedure

Follow the steps below to purchase a FlexusL instance.

1. Log in to the FlexusL **console**.
2. Click **Buy FlexusL** and specify parameters for the FlexusL instance.



Parameter	Description
Region	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. **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.
Image	FlexusL provides **OS images**, a rich variety of **application images**, and **private images** for you to select. Before using a private image, you need to learn about the **restrictions on private images of FlexusL instances** first and then create a private image. For details, see **Images Supported by FlexusL Instances**.

Parameter	Description
Instance specifications	You can select instance specifications based on your service requirements. Outbound traffic exceeding the traffic package is billed. For details, see **Billing**. **NOTE** 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.
(Optional) Instance name	You can customize your instance name. 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.
(Optional) Associated service resources	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). **NOTE** If you do not select **Data Disk (EVS)** during the purchase process, you can purchase it afterwards at the same price.
Required duration	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew is enabled by default, which means the purchased FlexusL instances will be automatically renewed before they expire. If you do not enable auto-renew during the purchase process, you can still enable it later after the instances are created. • Monthly subscription: auto-renews for 1 month every time • Yearly subscription: auto-renews for 1 year every time For details about auto-renewal, see **Auto-Renewal Rules**.
Quantity	Set the number of FlexusL instances to be purchased.

3. Click **Buy Now**.

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

> **CAUTION**
>
> After a FlexusL instance is created using an application image, wait until **the image with the pre-installed application is up and running**. Then, you can perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the installation may fail and you cannot log in to the image application dashboard.

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.

FAQs

- If you use a Linux private image to create a FlexusL instance and the private 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. As a result, the password reset function is unavailable. To install the plug-in, refer to the following:
  - **What Should I Do If the Password Cannot Be Reset After I Use a Private Linux Image to Create a FlexusL Instance or Change the OS of an Existing Instance and I Forgot the Initial Password of the Private Image?**
  - **What Should I Do If the Password Cannot Be Reset After I Use a Private Linux Image to Create a FlexusL Instance or Change the OS of an Existing Instance and I Know the Initial Password of the Private Image?**
- If you use a private image to create an HECS L 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 an L Instance or Change the OS of an Instance?**

2 Remotely Logging In to a FlexusL Instance

2.1 Login Modes

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 2-1 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 Linux FlexusL Instance 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. • 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)**	

Cloud OS	Local OS	Login Mode	Requirement
	Linux	Use commands. The method is the same as logging in to an ECS. • 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)**	
	Windows	You can remotely log in to a FlexusL instance through the management console. For details, see **Logging In to a FlexusL Instance 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 2-2 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.

Cloud OS	Local OS	Login Mode	Requirement
	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)**	
	Windows	You can remotely log in to a FlexusL instance through the management console. For details, see **Logging In to a FlexusL Instance Using VNC**.	No EIPs are required.

NOTE

If your login fails, refer to the following FAQ for troubleshooting. If your login fails, record the resource information and the time when the fault occurred, and **submit a service ticket** for technical support.

FAQs

- **What Can I Do If I Forget the Login Password of a FlexusL Instance?**
- **What Are the Default Username and Password for Logging In to a FlexusL Instance?**

2.2 Logging In to a FlexusL Instance Using VNC

Scenarios

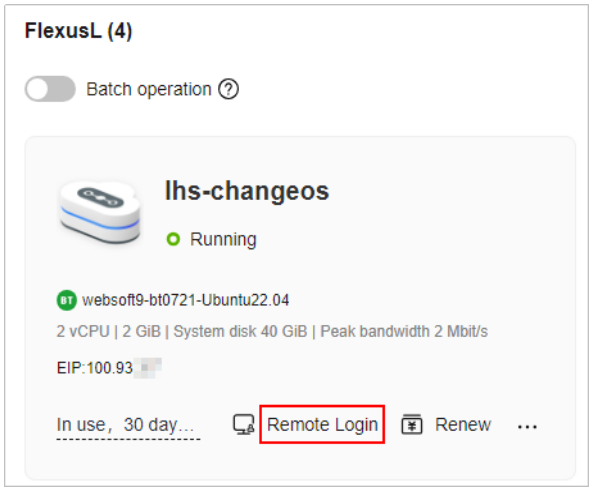
This section describes how to use VNC provided on the console to log in to a cloud server.

Notes and Constraints

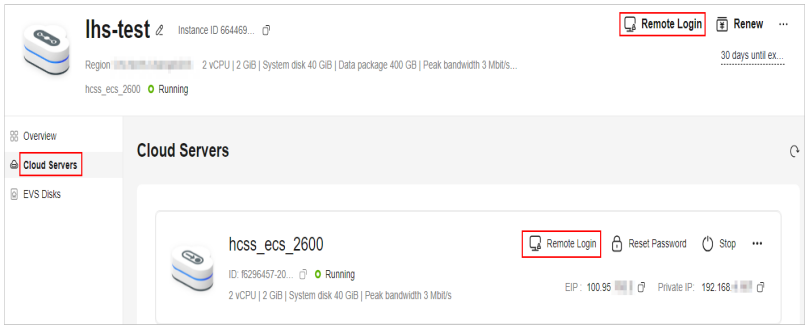
- You can only log in to a cloud server in the **Running** state.
- FlexusL instance servers do not have login passwords by default. When you log in to the server for the first time, **set a password**.

Procedure

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**.

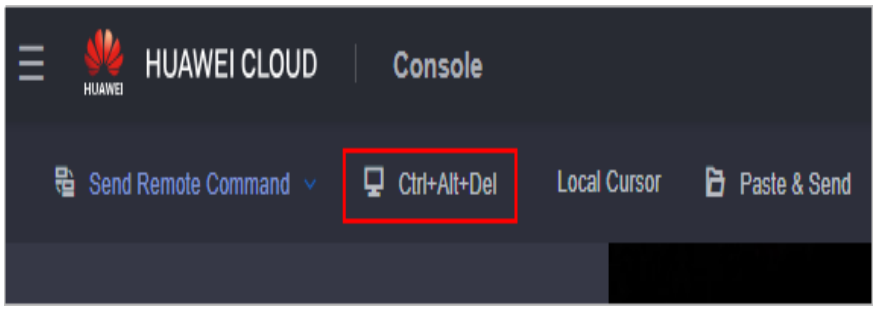


3. Log in to the FlexusL instance following the instructions.

   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.

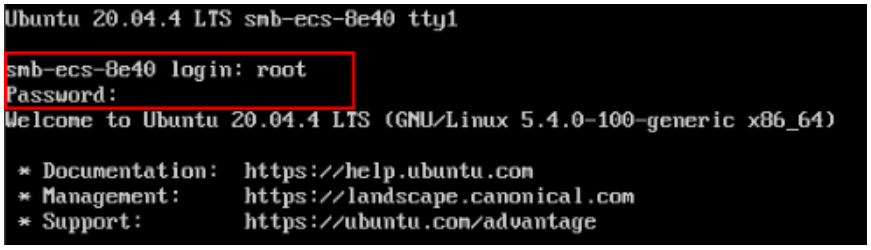
   - For Windows: Click **Ctrl+Alt+Del** to unlock the desktop and enter the password.

     The default username is **Administrator**.



- For Linux: Enter the username and password following the instructions.

  The default username is **root**.



2.3 Logging In to a Linux FlexusL Instance 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 for a FlexusL Instance**.

  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 2-1 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**.

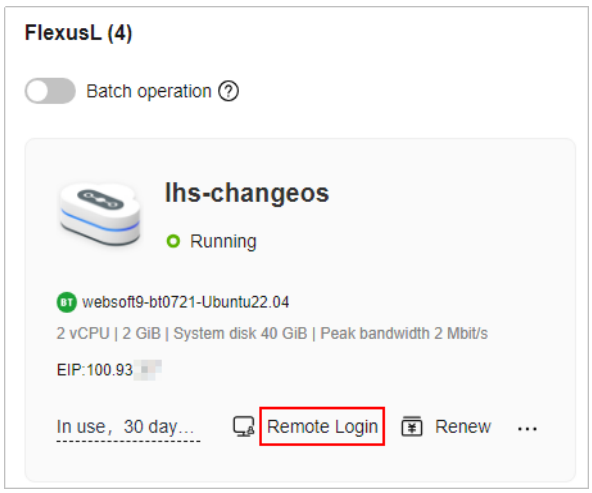
  ii. Add the user to the user group. For details, see **Adding Users to or Removing Users from a User Group**.

  NOTE

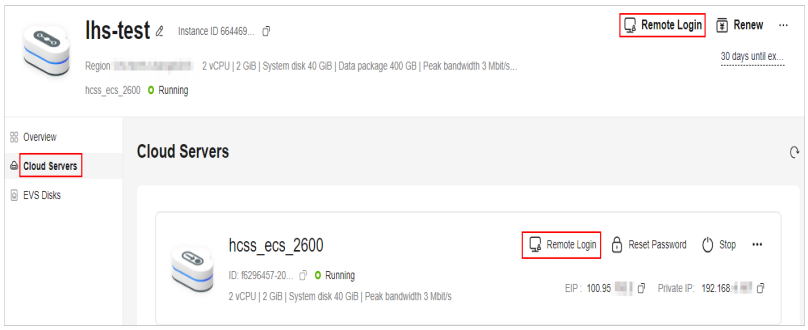
  When you use CloudShell to remotely connect to an ECS through a public network, service authorization is not required.

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**.



3. In the displayed dialog box, click **Log In via CloudShell** in the **CloudShell Login** area.
4. 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

      i. Configure parameters for logging in to the cloud server.

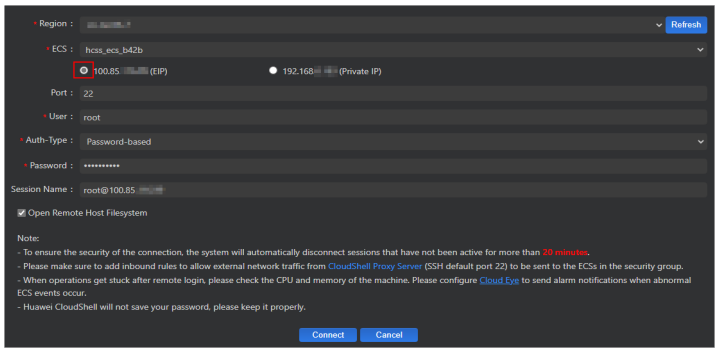


Table 2-3 Parameters for logging in to the cloud server

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 for a FlexusL Instance**.
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**.

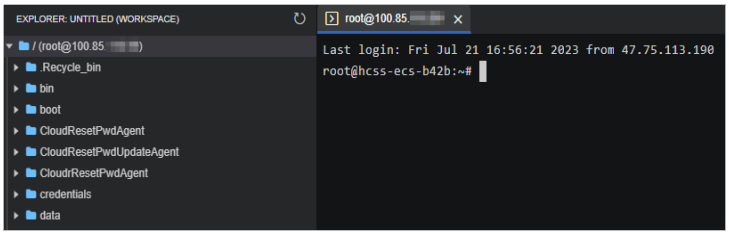
Parameter	Description
Session Name	The default format is *Username@IP address*. You can change it as needed.

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.

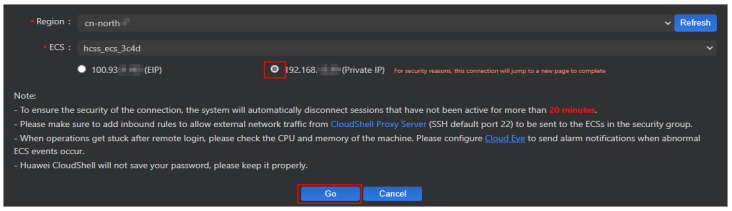
After the connection is successful, a figure similar to the following is displayed:

Figure 2-2 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 the **Prerequisites** first.

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

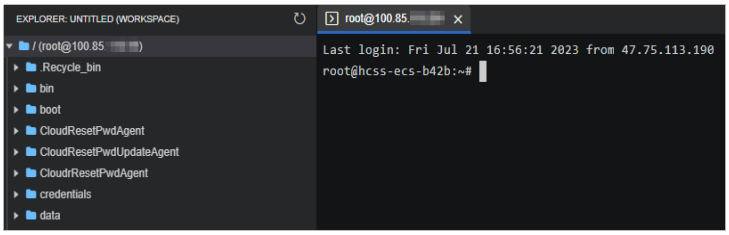
The configuration method using a private IP address is the same as that using an EIP. For details, see **Table 2-3**.

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 2-3 Successful login



3 Managing FlexusL Instances

3.1 Resetting the Password for a FlexusL Instance

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

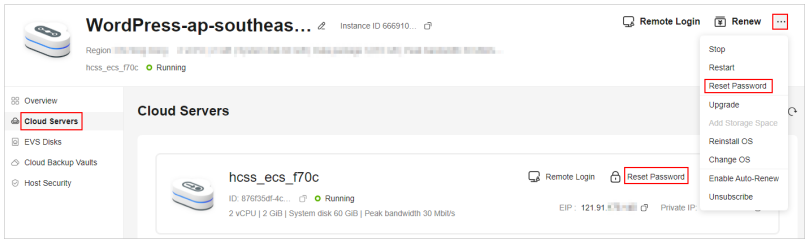
- You can reset the password only when the server is in **Stopped** or **Running** state. If you reset the password when the server is in **Running** state, the password change will be applied only after the server is restarted.
- The one-click password reset plug-in must have been installed.

  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:

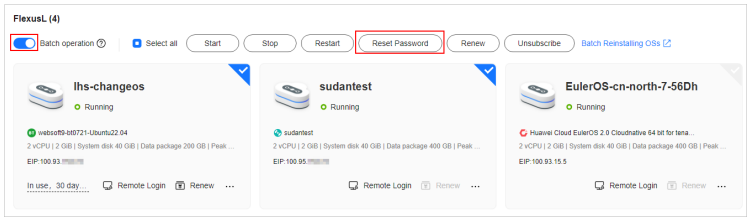
- In the **FlexusL** area, locate the target instance and choose ··· > **Reset Password**.
- Click the target instance name. On the displayed page, choose ··· > **Reset Password** in the upper right corner.
- Click the target instance name. In the left navigation pane, choose **Cloud Servers** and click **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 3-1 Reset a password

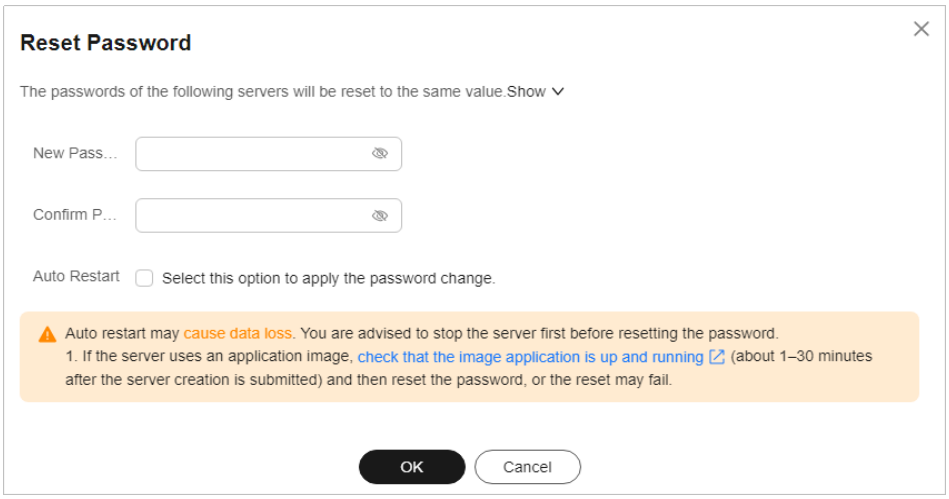


Table 3-1 Password complexity requirements

Parameter	Requirement
Password	• Consists of 8 to 26 characters. • Contains at least three of the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters for Windows ECSs: !@$%^-_=+[{()}]:,./?~#* – Special characters for Linux ECSs: !@$%^-_=+[{}]:,./?~#* • 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.)

4. 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.

3.2 Managing OSs of FlexusL Instances

3.2.1 Reinstalling the OS of a FlexusL Instance

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 of FlexusL Instances**.

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.

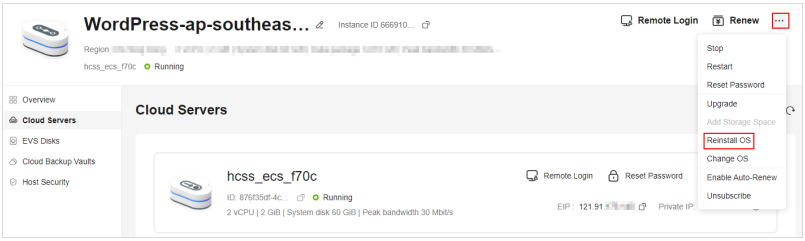
- The server will automatically restart after the OS is reinstalled, and only custom settings (such as the DNS) will be reset.

Billing

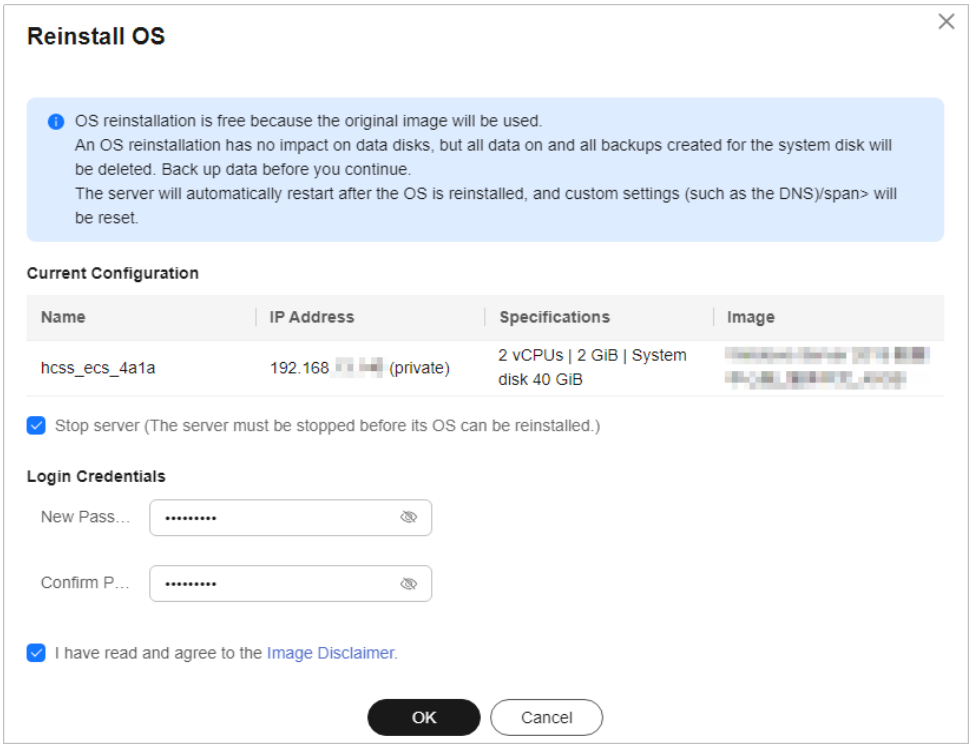
OS reinstallation is free because the original image will be used.

Procedure

1. Log in to the FlexusL **console** and click a resource card to go to the instance details page.
2. 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.



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.

3.2.2 Batch Reinstalling OSs of FlexusL Instances

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:

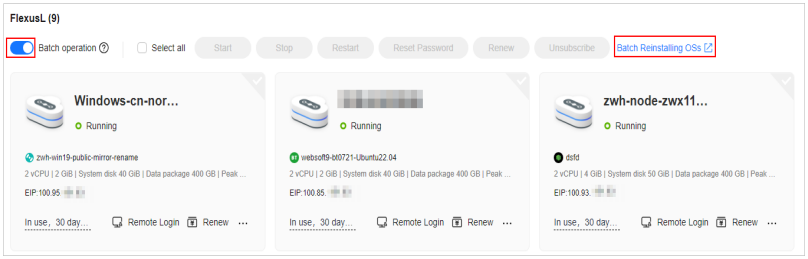
1. Prepare the COC FullAccess permissions.
   - If you are using a Huawei Cloud account, it has the COC FullAccess permissions by default. You can skip this step.
   - If you are an IAM user, a message is displayed, indicating that you do not have the required permissions. The account administrator needs 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 Cloud Operations Center (COC) console.

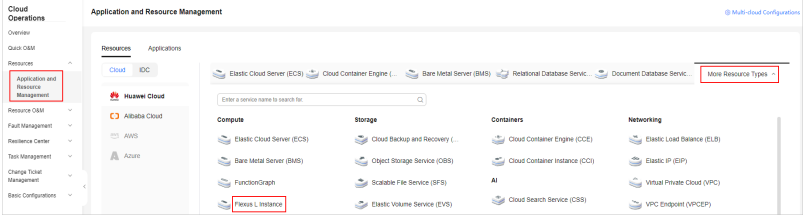
   You can also directly access the **COC** console. If a message is displayed indicating that you do not have the required permissions or need to apply for the OBT, perform the operations described in **Preparations** first.



2. Synchronize FlexusL instance resources to the COC console.

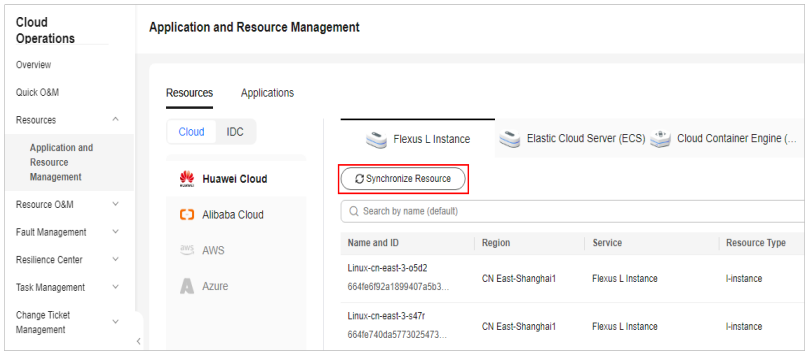
   Before batch reinstalling OSs, you must synchronize FlexusL instance resources to COC. The COC obtains the synchronized resources and then can reinstall OSs for the obtained FlexusL instances. Once new FlexusL instances are created, you must synchronize their resources to the COC console so that you can reinstall their OSs in batches on the COC console.

   a. On the COC console, in the navigation pane on the left, choose **Resources** > **Application and Resource Management**. On the **Application and Resource Management** page, choose **More Resource Types** > **Compute** > **Flexus L Instance**.

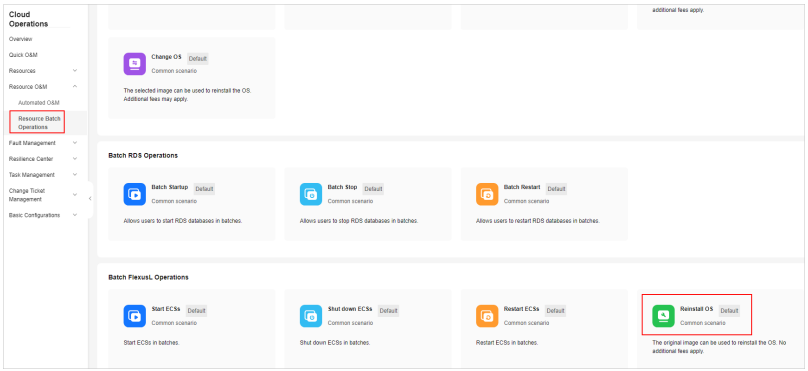


b. On the **Flexus L Instance** tab, click **Synchronize Resource**.

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

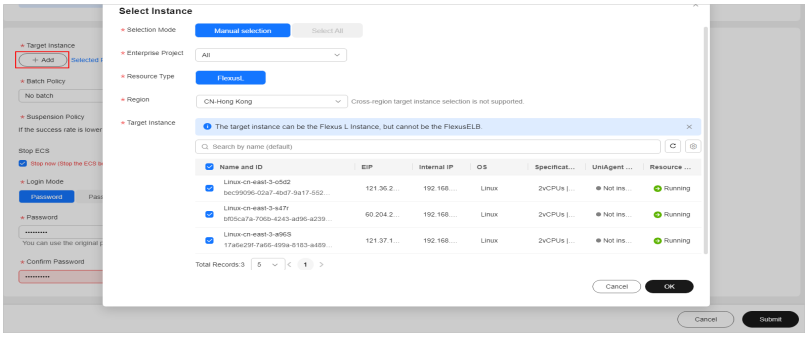


3. In the navigation pane on the left, choose **Resource O&M** > **Resource Batch Operations**. In the **Batch FlexusL Operations** area, click **Reinstall OS**.



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

Figure 3-2 Batch reinstalling OSs



Parameter	Description
Target Instance	• **Selection Mode**: **Manual selection** (only this option supported) • **Enterprise Project**: **All** • **Resource Type**: fixed to **FlexusL**, 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	Select a batch policy based on your requirements. • **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 will be executed in the same batch. **NOTE** • 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	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. Success rate = (Number of FlexusL instances whose OSs are successfully reinstalled/Total number of FlexusL instances) x 100%
Stop ECS	This option is displayed when there are FlexusL instances in **Running** state. Select **Stop now**.
Login Mode	• **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. **NOTE** Currently, FlexusL instances do not support password pairs.

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

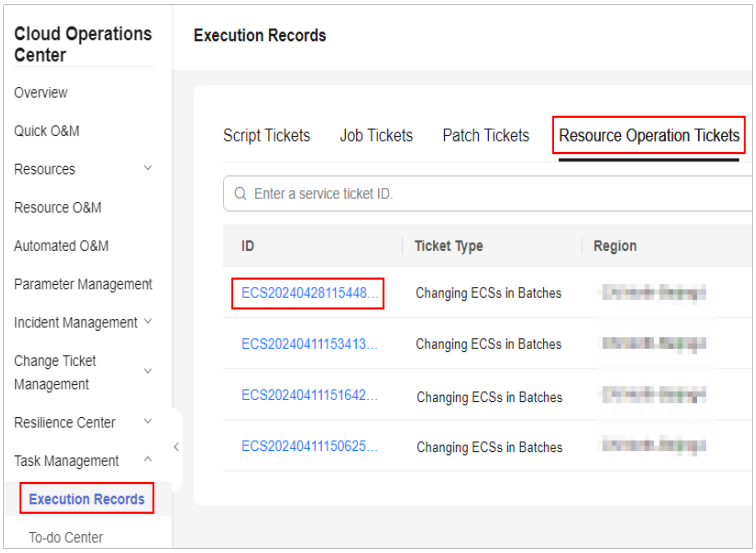
   After the OS is reinstalled, the cloud server will automatically restart. When the server status is **Running**, the OS reinstallation is complete.

   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

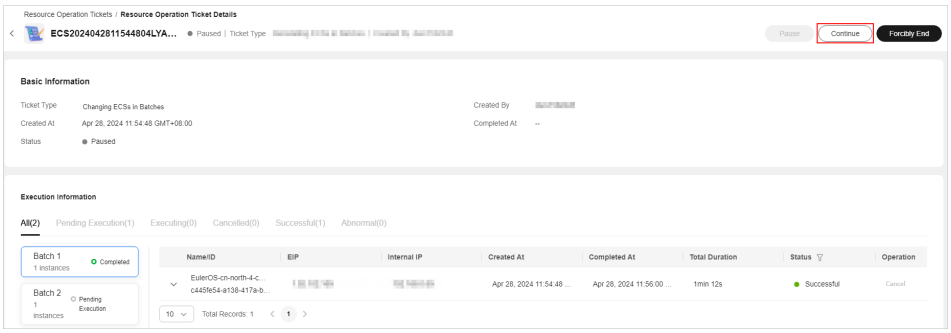
If you select **Automatic** or **Manual** and multiple batches of OS reinstallation tasks are generated, the process will be suspended after each batch of tasks is executed. Perform the following operations to manually continue the next batch of tasks:

1. Log in to the **COC** console.
2. Choose **Task Management** > **Execution Records**. On the **Resource Operation Tickets** tab, click the target service ticket ID.



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

Figure 3-3 Service ticket details



3.2.3 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 reset the password of, restart, or stop the FlexusL instance immediately after the OS is changed. Wait for several minutes until the system successfully injects the password, or the login will fail.

Constraints

- Application images have the minimum CPU and memory specification requirements. If the specification of a FlexusL instance is low, you cannot change its OS using an application image. For example, you cannot change the OS of a FlexusL instance with 2 vCPUs and 4 GiB memory to the GitLab application image that needs to use at least 2 vCPUs and 8 GiB memory. To do so, **upgrade the FlexusL instance** first and try again.
- After the OS is changed, the login password is cleared. You need to **reset the password** for logging in to the new OS. 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.
- Restrictions on private images of FlexusL instances are as follows.

Table 3-2 Restrictions on private images of FlexusL instances

Item	Description
Region	The FlexusL instance and the private image must belong to the same region. Otherwise, the image cannot be used to create the FlexusL instance. Therefore, before creating a FlexusL instance from a private image, create a private image in the region where the target FlexusL instance resides.
Server architecture	Only x86 is supported.

Item	Description
Image type	Only system disk images are supported. Data disk images and full-servers images are not supported. • Linux system disk images only support the following image sources: free public Linux images provided by Huawei Cloud, images created from FlexusL instances that are created using application images, and third-party private images you have imported. Other billed Linux images created from KooGallery images are not supported. • Windows system disk images with the Bring Your Own License (BYOL) license are supported. **NOTE** FlexusL instances do not support full-server images. If you want to migrate an entire server to a FlexusL instance, use Server Migration Service (SMS). For details, see **Migrating Servers Using Server Migration Service (SMS)**.
Password reset plug-in	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 existing FlexusL instance because 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?**

Preparations

Before using a private image to change the OSs of multiple FlexusL instances, use **Image Management Service (IMS)** to create an image first.

CAUTION

Before creating images, make sure you have learned about the **restrictions on private images of FlexusL instances**.

Table 3-3 Creating an image using IMS

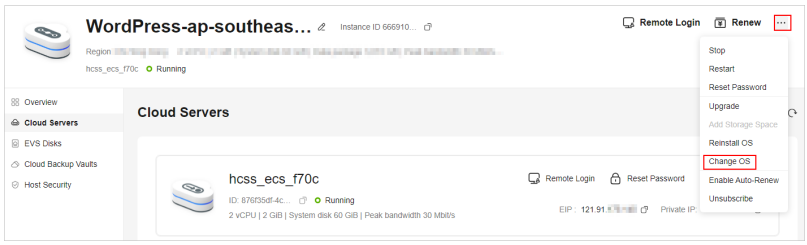
Scenario	Description	Related Operations
Scenario 1	If your private image is created from a FlexusL instance, FlexusX instance, or ECS, it can be used in the current region. If you want to use the private image in another region, replicate the image to the region where you want to use it first.	• **Creating a System Disk Image from a Windows ECS** • **Creating a System Disk Image from a Linux ECS** • **Replicating Images Across Regions**
Scenario 2	If your private image is created on another cloud platform or downloaded from a third party, import the private image using IMS. Refer to the operation guide based on the image file format: • External image files can be in any of the following formats: VMDK, VHD, QCOW2, RAW, VHDX, QED, VDI, QCOW, ZVHD2, and ZVHD. • ISO files.	• **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	If you want to use a private image of another Huawei account, ask the account owner to share the image with you and replicate the shared image as a private image.	• **Sharing Images** • **Replicating a Shared Image**

Billing

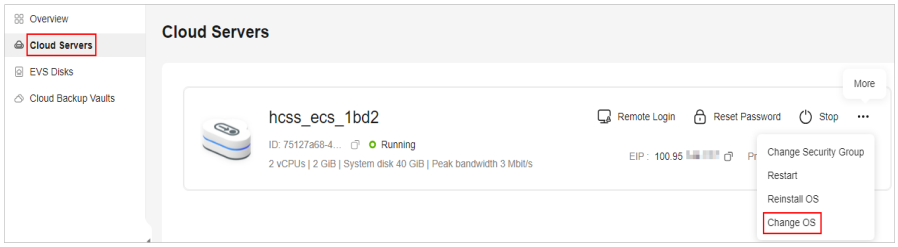
An OS change does not involve refund or supplementary payment.

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.



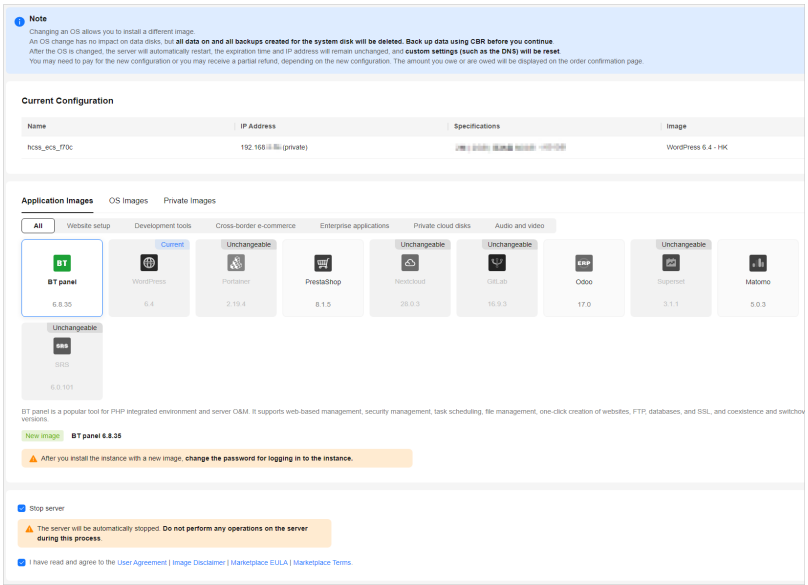
- Method 3: On the **Cloud Servers** page, choose ··· > **Change OS** in the row containing the target server.



- 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.

     FlexusL provides **OS images**, a rich variety of **application images**, and **private images** for you to select. Before using a private image, you need to learn about the **restrictions on private images of FlexusL instances** first and then create a private image. For details, see **Images Supported by FlexusL Instances**.
   - Select **Stop server**. The server must be stopped before its OS can be changed.



4. Read and agree to the agreements, and click **Submit**.

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

NOTICE

- Do not reset the password of, restart, or stop the FlexusL instance immediately after the OS is changed. Wait for several minutes until the system successfully injects the password, or the login will fail.
- After the OS is changed, the login password is cleared. You need to **reset the password** for logging in to the new OS. 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.

FAQs

- If you use a Linux private image to change the OS of a FlexusL instance and the private 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. As a result, the password reset function is unavailable. To install the plug-in, refer to the following:
  - **What Should I Do If the Password Cannot Be Reset After I Use a Private Linux Image to Create a FlexusL Instance or Change the OS of an Existing Instance and I Forgot the Initial Password of the Private Image?**
  - **What Should I Do If the Password Cannot Be Reset After I Use a Private Linux Image to Create a FlexusL Instance or Change the OS of an Existing Instance and I Know the Initial Password of the Private Image?**
- If you use a private image to change the OS of an HECS L 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 an L Instance or Change the OS of an Instance?**

3.3 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 3-4 Unsupported upgrade

Instance Specifications	vCPUs | Memory	System Disk	Peak Bandwidth	Data Package
Current	2 vCPUs | 8 GiB	120 GiB	10 Mbps	2,000 GB
New	4 vCPUs | 8 GiB	180 GiB	6 Mbps	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

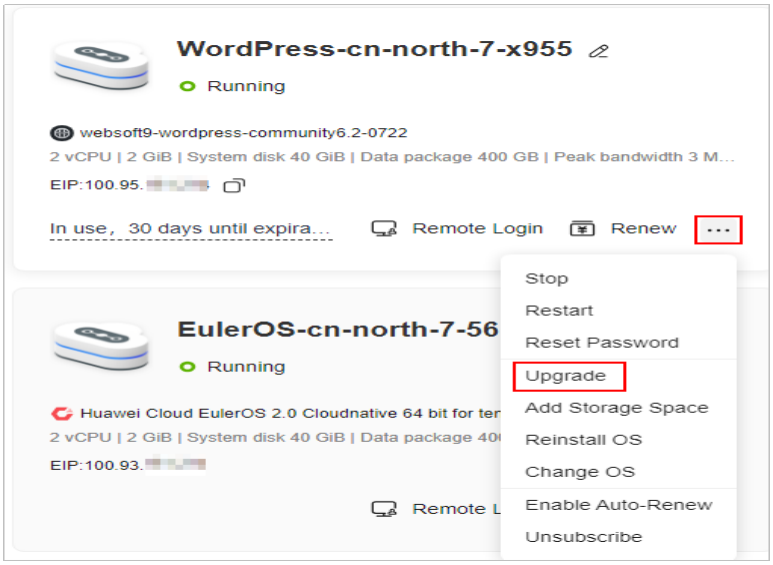
When upgrading specifications, you need to pay the difference in price. For details, see **Pricing of a Changed Specification**.

Preparations

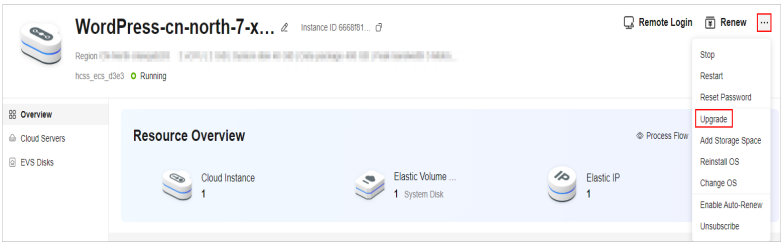
An upgrade failure may result in lost server data. You are advised to back up the data using CBR before you continue. For details, see **Method 2: Manual Backup**.

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.

3.4 Viewing Details of a FlexusL Instance

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.
Security	Servers scanned by HSS • : No risks detected. • : Risks detected. You can view risk details on the console.
Specifications	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: • 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: • View domain names. • Add, resolve, disable, or delete a domain name. For details, see **Managing Domain Names**.
Security Groups	On the **Security Groups** tab, you can: • View inbound and outbound security group rules. • Change the security group. For details, see **Changing the Security Group of a FlexusL Instance**. • Configure security group rules. For details, see **Configuring Security Group Rules for a FlexusL Instance**.
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: • View network interface details, including the ID, EIP, private IP address, security group, and MAC address. • Change the security group. For details, see **Changing the Security Group of a FlexusL Instance**.

3.5 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 3-4 Property and value

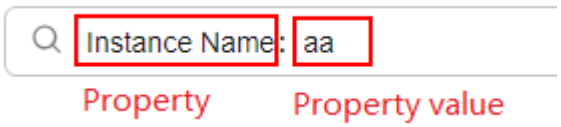


Table 3-5 describes each property.

Table 3-5 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.
Server ID	ID of the cloud server in a FlexusL instance. Figure 3-5 shows the instance ID and cloud server ID on the FlexusL console. **Figure 3-5** Instance ID and cloud server ID 
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.

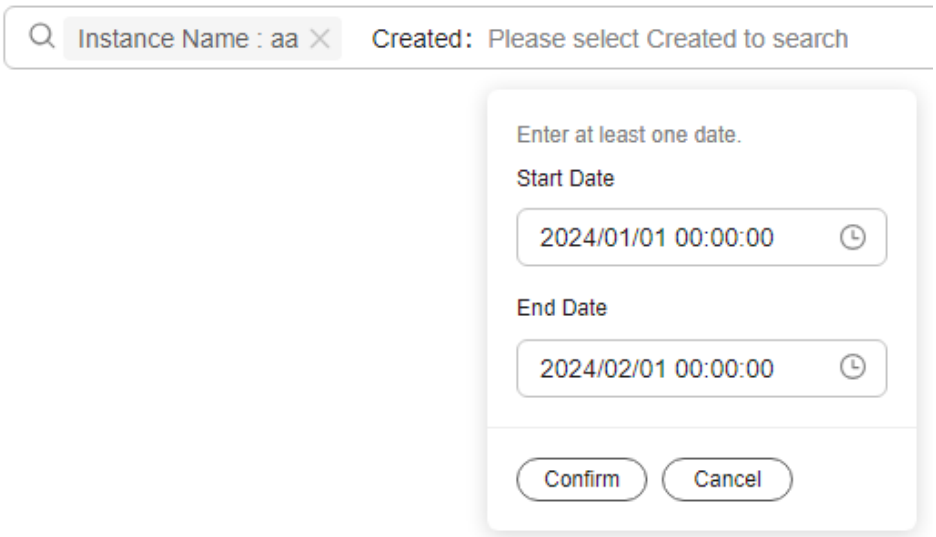
- Example 3: Searching by multiple properties with multiple values
  You can search by multiple properties and the properties are in AND relationship.

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.



4 Managing Images

4.1 Overview

Image Types

FlexusL provides OS images, application images, and private images for you to choose from.

Image Type	Description
OS Images	OS images only include the necessary OSs to launch servers, without any application data or environment configurations. After a FlexusL instance is created from an OS image, it runs on an OS without any applications installed. You can install applications based on your service requirements. For details about how to create a FlexusL instance from an OS image, see **Creating an Nginx Server Using the CentOS Image**.
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. For details about operations on application images, see **Managing FlexusL Application Images**.
Private Images	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)**.

OS Images

The following table lists the OS images supported by FlexusL.

Image Name	Description
Huawei Cloud EulerOS	Huawei Cloud EulerOS (HCE OS) is a Linux distribution based on the open-source community openEuler developed by Huawei. It provides a cloud-native, high-performance, secure, and stable execution environment for developing and running applications.
CentOS	CentOS is a popular open-source Linux distribution based on Red Hat Enterprise Linux (RHEL) source code.
Ubuntu	Ubuntu is a popular Linux distribution based on Debian. It is free, stable, easy to use, and has a vast array of community resources available.
Debian	Debian is a stable, convenient Linux distribution. It provides a more powerful software package management tool than most Linux distributions and is one of the preferred OSs for website building.

Application Images

The following table lists the application images supported by FlexusL. The supported application images vary depending on the region. For details, see the applications images displayed on the management console.

For details on how to perform operations on application images, see **Managing FlexusL Application Images**.

Image Name	Description
WordPress, an enterprise website setup system	WordPress was initially a blogging platform, but it gradually evolved into a free content management system (CMS) and website setup platform. It has earned a reputation for ease of use, scalability (plug-ins, templates, and secondary development), powerful functions, and friendly search engines.
BT panel, a visual Linux panel	BT panel is a popular tool for PHP integrated environment management and server O&M. It supports web-based management, security management, task scheduling, file management, one-click creation of websites, FTP, databases, and SSL, and coexistence and switchover of multiple PHP versions.

Image Name	Description
Odoo, an enterprise ERP system	Odoo is a global open-source ERP/CRM software developed using Python and PostgreSQL and has more than 730 partners and 2 million users. It has a powerful, flexible system architecture that enables fast iteration. The version difference lies in the user interface and functional modules. You can modify, upgrade, and add functions in modules without modifying the core code. Common modules include procurement management, sales management, inventory management, financial management, goods management, marketing management, customer relationship management, production management, personnel management, service support, e-commerce, and website building. Odoo is great for industries like manufacturing, retail chain, e-commerce, and international trade.
PrestaShop, an e-commerce system	PrestaShop is an open source e-commerce platform written in the PHP programming language with support for the MySQL database management system. More than 40,000 online stores around the world have been deployed using Prestashop. Prestashop uses Smarty for programming and is highly scalable. It supports multiple languages, currencies, and payment methods. Prestashop is a good choice for international trade websites.
Superset, a data exploration and visualization platform	Apache Superset (formerly known as Panoramix and Caravel) is an open-source data analysis and visualization platform. This tool provides a quick way to intuitively visualize datasets by allowing you to create and share interactive dashboards. It is also an enterprise-level intelligent business web application.
Portainer, a Docker visual runtime environment	Portainer is a graphical management tool for Docker. It is compiled using GO and offers a range of functions such as status display, quick deployment of application templates, basic operations on Docker (containers, images, networks, and database logical volumes), log display, and a container console.
Nextcloud, an enterprise cloud disk	Nextcloud is an open-source cloud storage software for self-built private web disks. It was developed using PHP and MySQL and provides multiple clients to support access from different devices. You can easily synchronize data with and share data stored on servers. You can also synchronize data from other sources such as Dropbox, FTP, OpenStack Object Storage, SMB, WebDAV, and SFTP.

Image Name	Description
GitLab, a one-stop DevOps platform	GitLab was initially an open source code repository management project designed to help teams collaborate on software development. Now it is a DevOps platform that provides a complete solution for software development and operations. GitLab delivers a range of functions, including project management, planning, creation, validation, packaging, release, configuration, monitoring, and protection of applications.
Matomo, a network statistics and analysis platform	Matomo is a powerful open-source network analysis platform that has full data ownership, while also helping ensure compliance with General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). Matomo's advanced search engine optimization and conversion optimization significantly improve your digital marketing capabilities, particularly for commercial software.
SRS, a real-time video server	SRS is a simple and efficient real-time video server that supports various real-time streaming media protocols, such as RTMP, WebRTC, HLS, HTTP-FLV, and SRT. Based on coroutine technology without async callback problem, SRS is also cloud native (docker image, k8s deploy, telemetry, metrics, etc). It is focused on real-time streaming gateways and supports streaming protocols such as RTMP, HLS, WebRTC, HTTP-FLV and SRT.
Joomla	Joomla is a website content management system (CMS) for enterprise websites and e-commerce. As one of the world's three most popular open source content management systems, Joomla is renowned for its flexibility and extensibility and excels in e-commerce.
Redmine	Redmine is a web-based project management application used to track requirements, defects, and other items. It provides project management, wikis, and Git integration.
Ghost	Ghost is a blog creation and paid reading platform. It is used in scenarios such as enterprise website creation. Ghost is a powerful app for professional publishers to create, share, and grow a business around their content.
Moodle	Moodle is an open-source online education system for global users and can be used to establish open course systems.
EspoCRM	EspoCRM is a web-based customer relationship management (CRM) system designed to help enterprises build and maintain strong customer relationships. It easy to customize and efficient to use.

Image Name	Description
KodCloud	Kodbox is an open-source enterprise net disk system that integrates online file management, multi-cloud storage, and collaborative office. It is commonly used for document collaboration and provides an experience similar to Windows.
Node.js runtime environment	The Node.js runtime environment comes with Node.js 21 pre-installed. You can obtain Node.js in just one click and quickly deploy Node.js applications.

Private Images

When you create FlexusL instances from private images, only x86 system disk images are supported. Data disk private images and full-server private images are not supported.

- Linux system disk images only support the following image sources: free public Linux images provided by Huawei Cloud, images created from FlexusL instances that are created using application images, and images you have imported. Other billed Linux images (such as UnionTech OS) provided by Huawei Cloud are not supported.
- Windows system disk images with the Bring Your Own License (BYOL) license are supported.

NOTE

FlexusL instances do not support full-server images. If you want to migrate an entire server to a FlexusL instance, use Server Migration Service (SMS).

For details, see **Migrating Servers Using Server Migration Service (SMS)**.

4.2 Managing FlexusL 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 1** describes how to initialize the application pre-installed in the image.

Table 4-1 Initializing the application pre-installed in the image

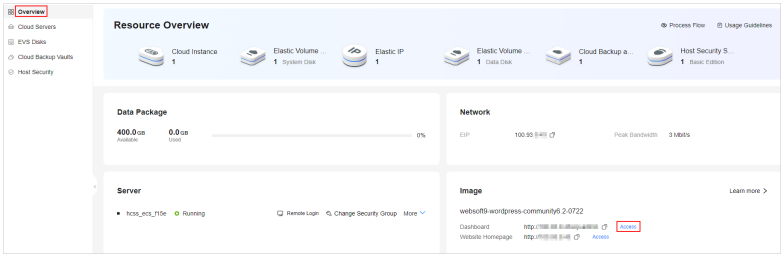
Application Image	Initialization
BT panel	**Initializing BT Panel**
WordPress	**Initializing WordPress**
Odoo	**Initializing Odoo**
Matomo	**Initializing Matomo**
Portainer	**Initializing Portainer**
GitLab	**Initializing GitLab**
Prestashop	**Initializing PrestaShop**
Superset	**Initializing Superset**
Nextcloud	**Initializing Nextcloud**
SRS	Initialization not involved.

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.


Overview
Cloud Servers
EVS Disks
Cloud Backup Vaults
Host Security
Resource Overview
Process Flow
Usage Guidelines
Cloud Instance
Elastic Volume
System Disk
Elastic IP
Elastic Volume
Data Disk
Cloud Backup a...
Host Security S...
Basic Edition
Data Package
400.0
Available
0.0
Used
0%
Network
EIP
Peak Bandwidth
3 Mbit/s
Server
Running
Remote Login
Change Security Group
More
Image
Learn more
websoft9-wordpress-community6.2-0722
Dashboard
Website Homepage
Access

5 Managing EVS Disks

5.1 Overview

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. For details about EVS disks, see **Disk Types and Performance**.

System Disks of FlexusL Instances

- System disks of FlexusL instances are General Purpose SSD EVS disks.
- Each FlexusL instance has one system disk with a fixed capacity. System disks of FlexusL instances cannot be expanded separately. You can expand the system disk capacity by upgrading the instance specifications. For details, see **Upgrading a FlexusL Instance**.
- System disks can only be purchased, renewed, and unsubscribed from along with the FlexusL instances they are attached to. They cannot be detached from instances.

Data Disks of FlexusL Instances

- Data disks of FlexusL instances are General Purpose SSD V2 EVS disks.
- Each FlexusL instance can have only one data disk. The disk size range is from 10 to 2048, in GiB. You can purchase a data disk when purchasing a FlexusL instance, or you can purchase one on the FlexusL console afterwards.
  - After a data disk is purchased, it is automatically attached to the FlexusL instance without manual intervention.

    A newly purchased data disk must be manually initialized before you can use it. For how to initialize a data disk, see **Initializing a Data Disk**.
  - Data disks (billed on a yearly/monthly basis) can only be renewed and unsubscribed from together with the FlexusL instances they are attached to. They cannot be detached from FlexusL instances.

- Data disks used by FlexusL instances only can be purchased on the FlexusL console. Existing EVS disks (including EVS disks attached to other servers) on the EVS console cannot be attached to FlexusL instances.

Notes and Constraints

- System disks of FlexusL instances cannot be expanded, attached, or detached, separately.
- Data disks of FlexusL instances can only be added or expanded on the FlexusL console, but cannot be detached. Existing EVS data disks cannot be attached to FlexusL instances.
- System and data disks of FlexusL instances cannot be renewed or unsubscribed from, separately.

5.2 Adding a Data Disk

Scenarios

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. If you have additional storage requirements, you can add data disks. You can purchase a data disk when purchasing a FlexusL instance, or you can purchase one afterwards. Data disks purchased on the FlexusL console are automatically attached to the FlexusL instances without manual intervention.

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

Constraints

- A FlexusL instance only supports one data disk. If there is already a data disk, no more data disks can be added.
- Data disks can be added only on the FlexusL console. You cannot add and attach data disks or attach existing data disks to FlexusL instances on the EVS console.
- Added data disks have the same expiration time as their FlexusL instances.
- After data disks are added to FlexusL instances, these disks cannot be detached or unsubscribed from separately.
- The data disk can only be added when the server is **Running** or **Stopped**.

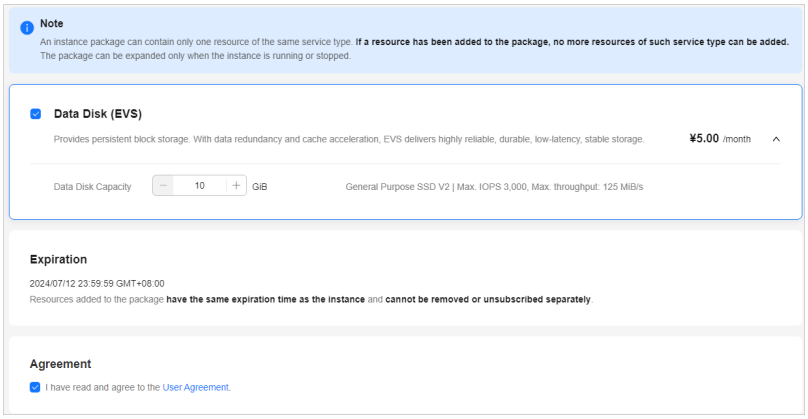
Billing

You need to pay for data disks. The unit price of the data disk purchased separately is the same as that of a data disk purchased along with a FlexusL instance.

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

- The added data disk is automatically attached to the FlexusL instance server without manual intervention.
- The added data disk must be manually initialized in the cloud server OS before you can use it. For how to initialize a data disk, 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.

5.3 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

You need to pay for the added data disk capacity. The unit price of the data disk expanded separately is the same as that of a data disk purchased along with a FlexusL instance.

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**.

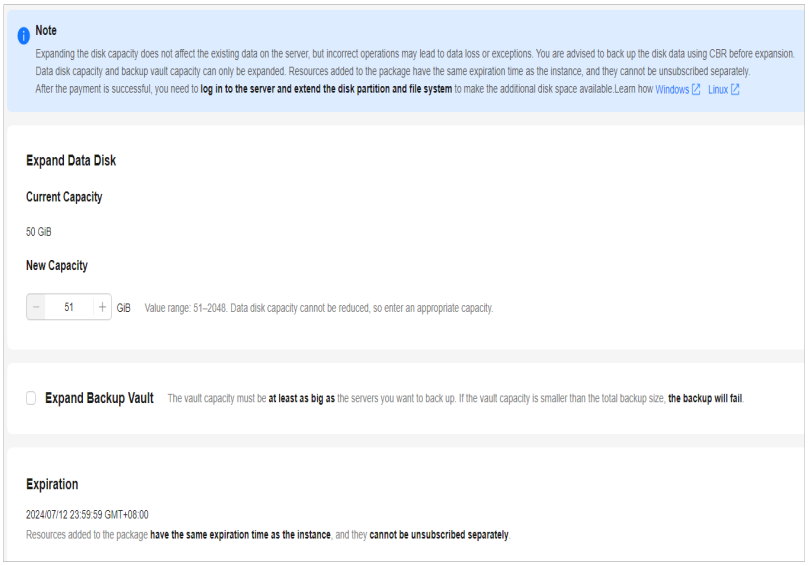
   Log in to the server and add the additional capacity to an existing partition or a new partition to make the additional capacity available for use.

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.



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 Windows, see **Extending Disk Partitions and File Systems (Windows)**.
- For Linux, see **Extending Partitions and File Systems for Data Disks (Linux)**.

6 Managing Server Security

6.1 Overview

If FlexusL instances are not protected, they may be attacked by viruses, resulting in data leakage or data loss. This section describes common measures to improve FlexusL instance security.

Security Protection

FlexusL instances can be protected externally and internally.

Table 6-1 Methods for improving FlexusL instance security

Type	Description	Protection Method
External security	DDoS attacks and Trojan horses or other viruses are common external security issues. To address these issues, you can enable Host Security Service (HSS) to protect your FlexusL instances.	• **Enabling HSS** • **Backing Up Data Periodically**
Internal security	Weak passwords and incorrect ports opening may cause internal security issues. Improving the internal security is the key to improving the instance security. If the internal security is not improved, external security solutions cannot effectively intercept and block various external attacks.	• **Enhancing the Login Password Strength** • **Improving the Port Security** • **Periodically Upgrading the OS**

Enabling HSS

HSS is designed to improve the overall security for cloud servers. It 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.

- You can enable HSS (basic edition) when purchasing a FlexusL instance. After the purchase, your instance is automatically protected.
- You can also enable HSS on the HSS console after the FlexusL instance is purchased.

For details about how to enable HSS, see **Configuring HSS for a FlexusL Instance**.

Backing Up Data Periodically

CBR enables you to back up FlexusL instances 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.

- You can enable CBR when purchasing a FlexusL instance. After the purchase, CBR automatically backs up the FlexusL instance based on the default backup policy.
- You can also enable CBR on the CBR console after the FlexusL instance is purchased.

For details, see **Backing Up a FlexusL Instance**.

Enhancing the Login Password Strength

To ensure the security of your FlexusL instance, you can set a strong login password by following these guidelines:

- Set a password which consists of at least 10 characters.
- Do not use easily guessed passwords (for example, passwords in common rainbow tables or passwords with adjacent keyboard characters). The password must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters.
- Do not use your username or any part of it, such as administrator, test, root, oracle, and mysql.
- Change the password at least every 90 days.
- Do not reuse the latest five passwords.
- Set different passwords for different applications. Do not use the same password for multiple applications.

Improving the Port Security

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 in this group.

You can configure security group rules to control access to or from specific ports. You are advised to disable high-risk ports and only enable necessary ports.

Table 6-2 lists some high-risk ports. Do not use these ports for your services.

Table 6-2 High-risk ports

Protocol	Port
TCP	42 135 137 138 139 444 445 593 1025 1068 1434 3127 3128 3129 3130 4444 4789 5554 5800 5900 9996
UDP	135~139 1026 1027 1028 1068 1433 1434 4789 5554 9996

Periodically Upgrading the OS

After a FlexusL instance is created, you need to maintain and periodically upgrade the OS. Officially released vulnerabilities will be published in **Security Notices**.

6.2 Configuring the Security Group for a FlexusL Instance

6.2.1 Overview

Security Groups

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.

When you create a FlexusL instance, the system automatically creates a default security group (sg-default-smb) and associates it with the instance. You can also create a security group based on service requirements and associate it with the instance. An instance can be associated with multiple security groups, and traffic to and from the instance is matched by priority in a descending order.

For more information about security groups, see **Security Group**.

Security Group Rules

A security group has inbound and outbound rules to control traffic that is allowed to reach or leave the instances associated with the security group.

- Inbound rules: control traffic to the instances in a security group.
- Outbound rules: control traffic from the instances in a security group to access external networks.

Each security group has default rules. For details, see **Table 6-3**. You can also customize security group rules. For details, see **Configuring Security Group Rules for a FlexusL Instance**.

Table 6-3 Default security group rules

Direction	Action	Type	Protocol & Port	Source/ Destination	Description
Inbound	Allow	IPv4	All	Source: sg-default-smb	Allows instances in the security group to communicate with each other over IPv4 protocols.
Inbound	Allow	IPv6	All		Allows instances in the security group to communicate with each other over IPv6 protocols.
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 FlexusL 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.

6.2.2 Configuring Security Group Rules for a FlexusL Instance

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 configuring security group rules for application images, see **Configuring Security Groups for FlexusL Application Images**.

Figure 6-1 Adding an inbound rule

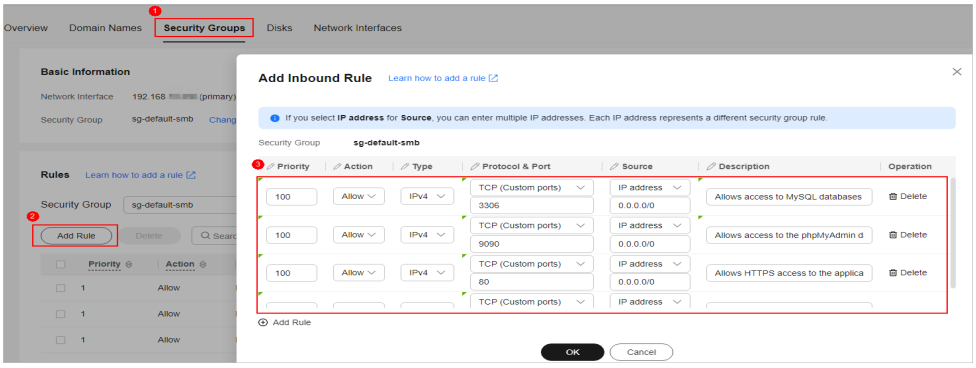


Table 6-4 Inbound rule parameter description

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
Action	Allow or Deny • 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. Deny rules take precedence over allow rules of the same priority.	Allow
Type	Source IP address version. You can select: • IPv4 • IPv6	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

Parameter	Description	Example Value
	Destination port used to match traffic in a security group rule. The value can be from 1 to 65535. Inbound rules control incoming traffic over specific ports to instances in the security group. Specify one of the following: ● 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	The source in an inbound rule is used to match the IP address or address range of an external request. The source can be: • **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. – 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	Supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

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

Table 6-5 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 • 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: • IPv4 • IPv6	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: • 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	The destination in an outbound rule is used to match the IP address or address range of an internal request. The destination can be: • **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. – 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	Supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

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 6-6**.

Table 6-6 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 6-2** is displayed, TCP port 80 is listened.

   Figure 6-2 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.

6.2.3 Changing the Security Group of a FlexusL Instance

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

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**.

6.2.4 Configuring Security Groups for FlexusL 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 for a FlexusL Instance**.

WordPress

Table 6-7 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	Specifies the internal forwarding port of application images
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.

BT Panel

Table 6-8 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.
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, Odoo, Nextcloud, and GitLab

Table 6-9 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	Specifies the internal forwarding port of application images
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M dashboard.

Portainer, Superset, and PrestaShop

Table 6-10 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: 80	0.0.0.0/0	Specifies the internal forwarding port of application images
1	Allow	IPv4	TCP: 3306	0.0.0.0/0	Allows access to MySQL databases.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M dashboard.

SRS

Table 6-11 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: 80	0.0.0.0/0	Specifies the internal forwarding port of application images
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.
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.
1	Allow	IPv4	TCP: 8000	0.0.0.0/0	Allows access to the WebRTC media server.

6.3 Configuring HSS for a FlexusL Instance

Scenarios

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

Item	Description
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

7 Managing Backups

7.1 FlexusL Backup Overview

Backup is a common method for server maintenance. FlexusL instances can back up data using multiple services, such as Cloud Backup and Recovery (CBR) and Image Management Service (IMS).

- **Cloud Backup and Recovery (CBR)** enables you to back up cloud servers and disks with ease. In the event 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.

  You can associate a backup vault with your cloud server when you purchase it on the FlexusL console. You can also enable CBR on the CBR console after the FlexusL instance is purchased.
- An image is a cloud server or disk template that contains an OS, service data, or necessary software. **IMS** allows you to manage the lifecycle of images.

  You create a system disk image for a FlexusL instance on the IMS console and use this image to restore the FlexusL instance. FlexusL instances can only be restored using system disk images, but not data disk images or full-server images.
- Data on FlexusL instances cannot be restored using snapshots.

NOTE

For the differences between backup and image, see **What Are the Differences Between Backup, Snapshot, and Image?**

This section describes how to back up FlexusL instance data using CBR.

How to Use CBR

- Scenario 1

  CBR is associated with FlexusL. You can associate a backup vault with your FlexusL instance when you purchase it on the FlexusL console. After a FlexusL instance is created with a CBR vault associated, CBR automatically backs up the entire FlexusL instance based on the default backup policy. Also, you can perform a manual backup at any time.

- Scenario 2

  If you do not associate a vault with the FlexusL instance during the purchase, you can buy a vault afterwards on the CBR console. For details, see **Creating a Cloud Server Backup**.

The comparison of the two scenarios is described in the following table. You can select one as required.

Table 7-1 Differences between cloud backup in the two scenarios

Scenario	Billing Mode	Lifecycle	Cloud Backup Types	Vault Capacity	Advantage
Scenario 1	Yearly/ Monthly (The validity period is the same as that of the FlexusL instance.)	For the CBR vault purchased along with the FlexusL instance on the FlexusL console, its lifecycle is the same as the FlexusL instance. It cannot be renewed or unsubscribed from separately, and cannot be disassociated from the FlexusL instance.	Cloud server backup	10 to 2,048, in GiB	Cheaper than the yearly/ monthly backup vault with the same duration purchased on the CBR console
Scenario 2	Yearly/ monthly and pay-per-use	For the CBR vault purchased on the CBR console, it has its own lifecycle. You can disassociate it from the FlexusL instance at any time.	Cloud server backup	10 to 10,485,760, in GiB	More flexible

Constraints

You can associate one CBR vault at most when you purchase a FlexusL instance on the FlexusL console. The CBR vault cannot be disassociated from the FlexusL instance after being purchased.

CBR Functions

Table 7-2 CBR functions

Function	Description
Backing Up a FlexusL Instance	After a CBR vault is associated with your FlexusL instance, you can apply a default backup policy or manually back up data.

Function	Description
Expanding the Backup Vault Associated with a FlexusL Instance	If the capacity of a cloud backup vault no longer meets your needs, you can expand the vault capacity.

7.2 Backing Up a FlexusL Instance

Scenarios

CBR enhances data integrity and service continuity. For example, if a FlexusL instance is faulty or a misoperation causes data loss, you can use backups to quickly restore data. This section describes how to back up a FlexusL instance.

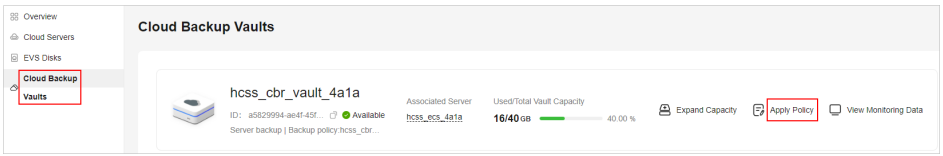
Prerequisites

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.

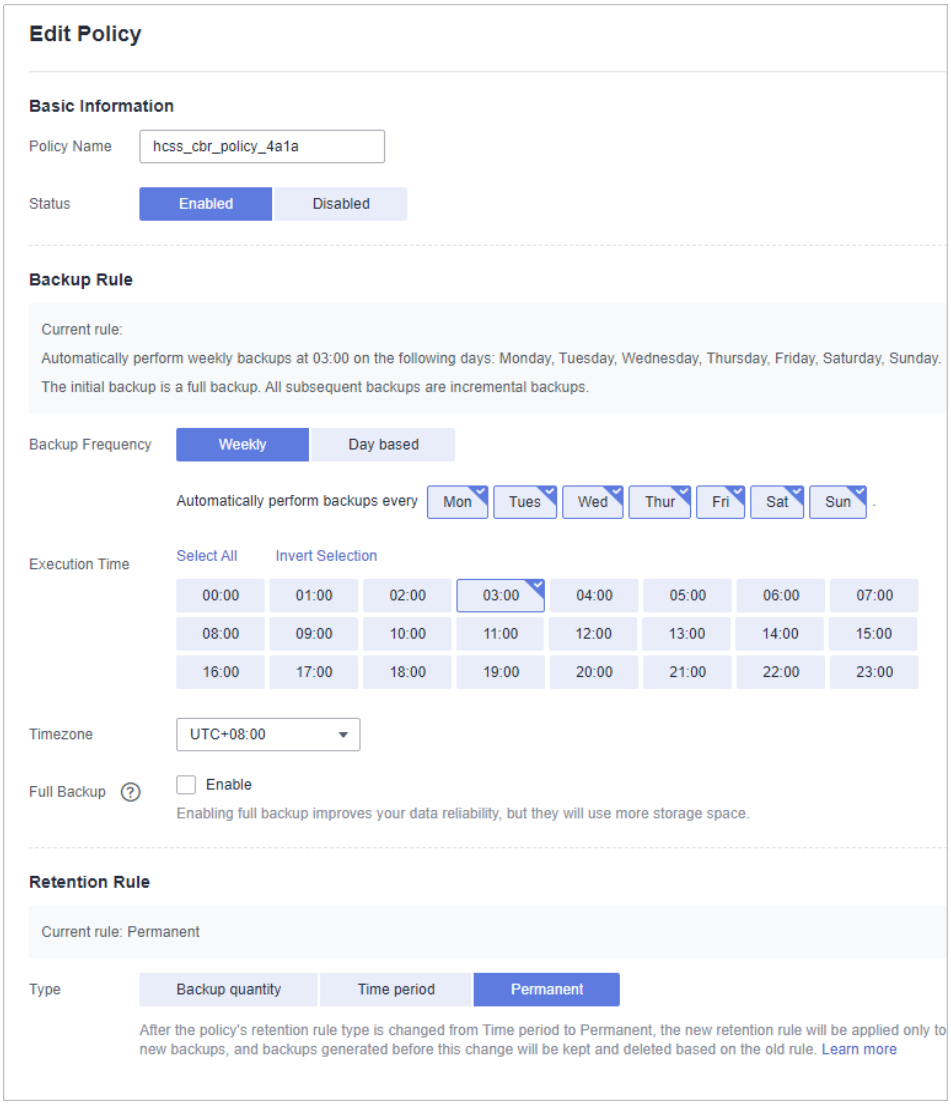
1. Log in to the FlexusL **console** and click a resource card to go to the instance details page.
2. On the displayed page, choose **Cloud Backup Vaults** from the left navigation pane and click **Apply Policy** in the upper right corner.



3. View or set the backup policy parameters.
4. 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.



5. Click **Create Now**.
6. After the backup policy is created, cloud servers are automatically backed up based on the policy.

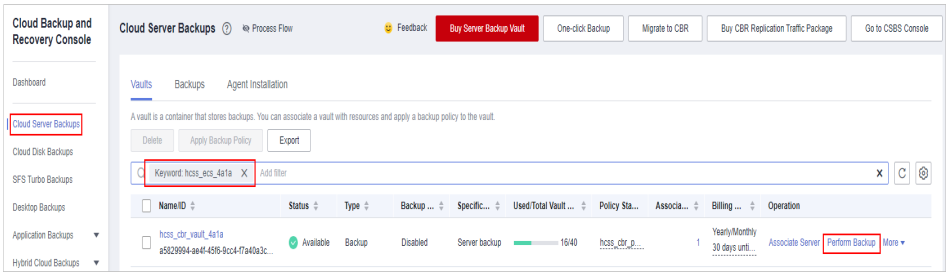
Method 2: Manual Backup

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.

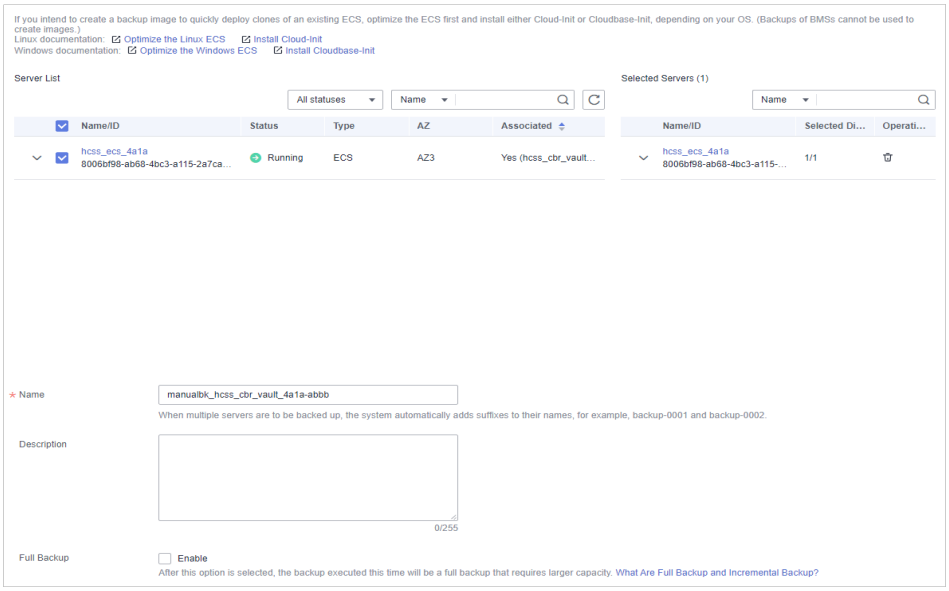
– If you associate a vault with a FlexusL instance server on the CBR console after the FlexusL instance is created, search by server ID.

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.



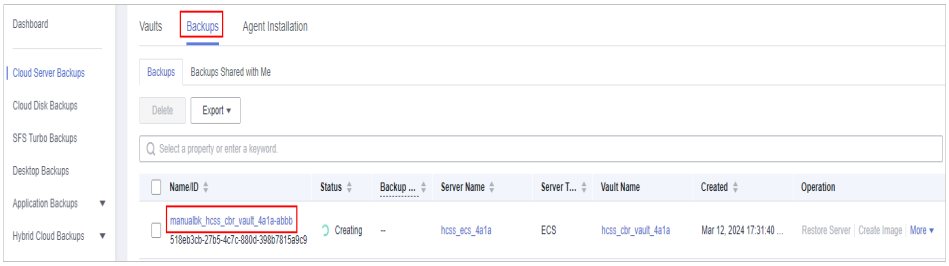
3. Set a backup name and determine whether to enable **Full backup**.

   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.



Follow-Up Operations

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**.

7.3 Expanding the Backup Vault Associated with a FlexusL Instance

Scenarios

Ensure that the capacity of the vault associated with the FlexusL instance is sufficient, or the backup will fail. You can expand the vault capacity as needed. This section describes how to expand the vault capacity on the FlexusL console. For details about how to expand the vault capacity on the CBR console, see **Expanding Vault Capacity**.

Constraints

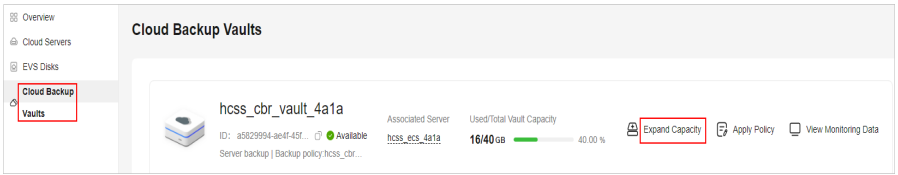
- The vault capacity can only be expanded. It cannot be reduced.
- The disk can only be expanded when the server is **Running** or **Stopped**.

Billing

The expanded capacity is billed.

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 GiB, the vault capacity must be greater than 80 GiB. 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.

8 Managing Domain Names

8.1 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.

8.2 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.

8.3 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

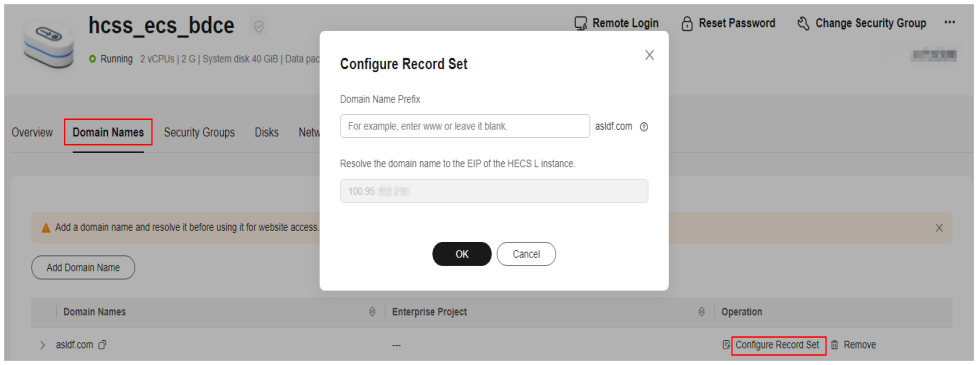
The domain name has been added.

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	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. Suppose the domain name is wpwebsite.com. • 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.
   - The new DNS server addresses will take effect within 2 to 24 hours, and the time may vary depending on the TTL value.

   – 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	Status of the domain name or subdomain. • **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.
Operation	• 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*.

9 Monitoring

9.1 Overview

Monitoring is important to ensure FlexusL instance performance, reliability, and availability. You can use Cloud Eye to monitor FlexusL instances and know their statuses. Cloud Eye can monitor a range of metrics, such as the CPU usage, disk usage, and bandwidth of FlexusL instances.

How Do I Use Monitoring?

After you purchase a FlexusL instance, Cloud Eye is enabled by default. It can monitor the cloud servers, EVS disks, and CBR vaults packaged in the FlexusL instances.

Cloud Server Monitoring

Server monitoring collects monitoring metrics at the OS layer of servers.

Server monitoring consists of basic monitoring, OS monitoring, and process monitoring. Basic monitoring does not require the Agent to be installed. OS monitoring and process monitoring require the Agent to be installed on the FlexusL instances to be monitored.

- Basic monitoring covers metrics automatically reported by FlexusL instances. The data is collected every 5 minutes. For details, see **Table 9-1**.
- OS monitoring provides proactive, fine-grained OS monitoring for FlexusL instances, and it requires the Agent to be installed on the FlexusL instances to be monitored. The data is collected every minute. In addition to the CPU usage, metrics such as memory usage can also be monitored. For details, see **OS Monitoring Metrics**.
- Process monitoring monitors active processes on FlexusL instances, and it requires the Agent to be installed on the FlexusL instances to be monitored. By default, Cloud Eye collects the CPU usage, memory usage, and the number of opened files of active processes.

Table 9-1 Basic monitoring metrics

Basic Monitoring Metric	Description
CPU Usage	CPU usage of the physical server accommodating the monitored cloud server (ECS), which is not accurate as that obtained from the ECS that is being monitored Unit: percentage (%) Formula: CPU usage of a cloud server (ECS)/Number of CPU cores on the cloud server (ECS)
Disk Read Bandwidth	Number of bytes read from the monitored object per second Unit: Byte/s Formula: Total number of bytes read from an EVS disk/Monitoring interval
Disk Write Bandwidth	Number of bytes written to the monitored object per second Unit: Byte/s Formula: Total number of bytes written to an EVS disk/Monitoring interval
Disk Read IOPS	Number of read requests sent to the monitored object per second Unit: Request/s Formula: Total number of read requests sent to an EVS disk/Monitoring interval
Disk Write IOPS	Number of write requests sent to the monitored object per second Unit: Request/s Formula: Total number of write requests sent to an EVS disk/Monitoring interval
Outband Incoming Rate	Number of incoming bytes received by the monitored object per second at the virtualization layer Unit: Byte/s Formula: Total number of outband incoming bytes on a cloud server (ECS)/Monitoring interval
Outband Outgoing Rate	Number of outgoing bytes sent by the monitored object per second at the virtualization layer Unit: Byte/s Formula: Total number of outband incoming bytes on a cloud server (ECS)/Monitoring interval

Basic Monitoring Metric	Description
Network Connections	Total number of TCP and UDP connections on a cloud server (ECS) Unit: Count
Server Inbound Bandwidth	Number of public and private byte received by the cloud server (ECS) per second Unit: Byte/s
Server Outbound Bandwidth	Number of public and private byte sent by the cloud server (ECS) per second Unit: Byte/s
Server Inbound PPS	Number of public and private packets received by the cloud server (ECS) per second Unit: Packet/s
Server Outbound PPS	Number of public and private packets sent by the cloud server (ECS) per second Unit: Packet/s
New Connections	Number of new connections (including TCP, UDP, and ICMP) created on the cloud server (ECS) Unit: connect/s

EVS Monitoring

EVS monitoring collects metrics of EVS disks every 5 minutes on average. For details, see **Viewing EVS Monitoring Data**.

CBR Monitoring

CBR monitoring collects metrics of the used vault size and vault usage of CBR every 15 minutes.

9.2 Viewing Monitoring Metrics of a FlexusL Instance

Scenarios

Cloud Eye monitors the cloud servers, EVS disks, and CBR vaults packaged in FlexusL instances. You can clearly view the monitoring metrics of FlexusL instances on the management console. Operations for viewing monitoring data of cloud servers, EVS disks, and CBR vaults are similar. This section shows how to view the metrics of the cloud server in a FlexusL instance.

Prerequisites

- A FlexusL instance is running properly.

  Cloud Eye does not display the monitoring data for stopped, faulty, or unsubscribed FlexusL instances. After such a FlexusL instance restarts or recovers, its monitoring data will be displayed on the Cloud Eye console.

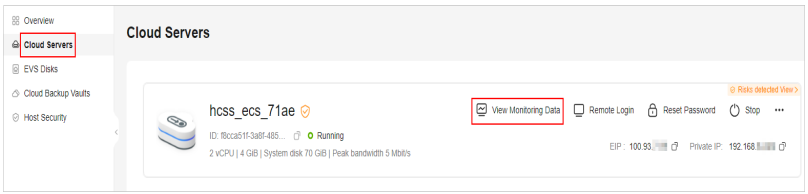
- The FlexusL instance has been running for a period of time.

  It takes a period of time to transmit and display the monitoring data. If your FlexusL instance is just created, wait for about 5 to 15 minutes and then view the monitoring data. The server and EVS monitoring data will be displayed in about 5 minutes and the CBR monitoring data will be displayed in about 15 minutes.

Procedure

1. Log in to the FlexusL**console**.
2. Click the target FlexusL resource card.

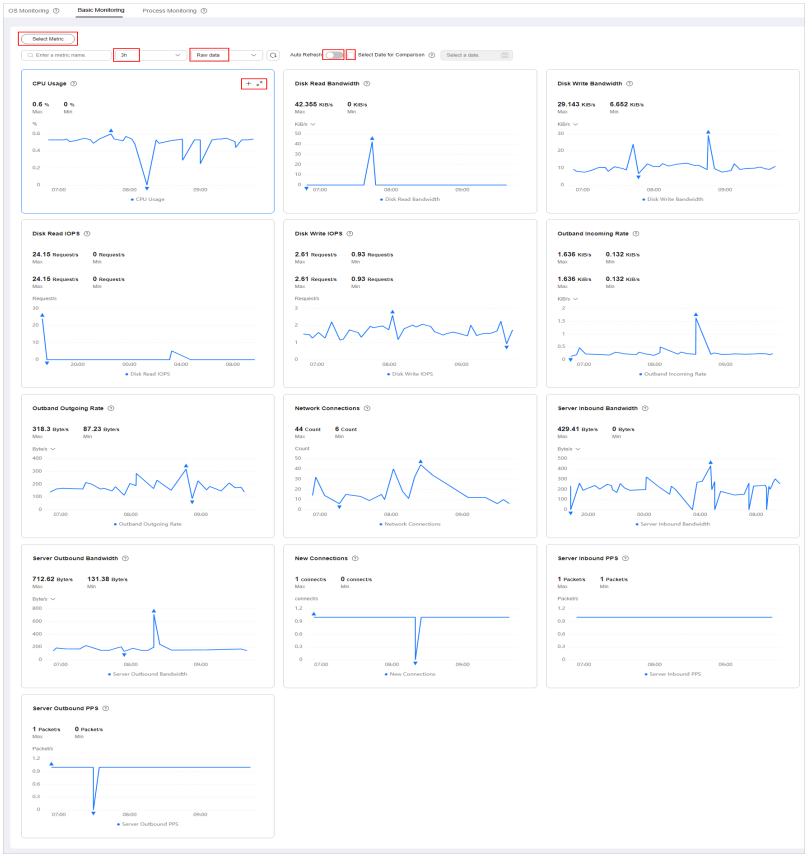
   Alternatively, enter the instance name, EIP, or server ID in the search box to filter the target FlexusL instance.
3. Choose **Cloud Servers** in the left navigation pane and click **View Monitoring Data**.

4. View basic monitoring metrics.
   - You can click **Select Metric** to select the monitoring metrics to be displayed.
   - You can view the curves of different metrics in the last 1, 3, or 12 hours, or last 1 or 7 days. You can also specify a time period.
   - You can determine whether to enable **Auto Refresh**. After this function is enabled, the system automatically refreshes data every 30 seconds.
   - You can determine whether to select **Select Data for Comparison** to compare the monitoring data in the current specified period with that in the same period on a specified date.

     For example, if you choose **3h**, select **Select Data for Comparison**, and specify the date to August 2, then the monitoring data in the last 3 hours is compared with that in the same period on August 2.
   - You can move the pointer to a metric graph and click  to create an alarm rule for the metric.

     For details, see **Creating an Alarm Rule to Monitor a Server**.
   - You can move the pointer to a metric graph and click  to zoom in the graph.



Related Operations

You can configure alarm rules for FlexusL instances to customize the monitored objects and notification policies. This enables you to learn about the statuses of FlexusL instances and receive notifications if there are any exceptions.

For details, see **Creating an Alarm Rule to Monitor a Server**.

