Flexus L Instance

User Guide

Issue	01
Date	2025-02-14

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Huawei Cloud Computing Technologies Co., Ltd.

Contents

1 Granting Permissions to Use FlexusL Instances Through IAM

FlexusL allows you to use **IAM** to implement fine-grained permissions control on your FlexusL resources. With IAM, you can:

- Create IAM users or user groups for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing FlexusL resources.
- Grant users only the permissions required to perform a given task based on their job responsibilities.
- Entrust a Huawei Cloud account or a cloud service to perform efficient O&M on your FlexusL resources.

If your Huawei Cloud account meets your permissions requirements, you can skip this section.

This section describes how to grant permissions to a user. **Figure 1-1** shows the process.

Prerequisites

Before assigning permissions to user groups, you should learn about system-defined policies supported by FlexusL and select the policies based on service requirements.

For details about the system-defined policies supported by FlexusL instances, see **System-defined policies for FlexusL instances**. For the permissions of other services, see **System-defined Permissions**.

Process Flow

Figure 1-1 Process for granting FlexusL instance permissions
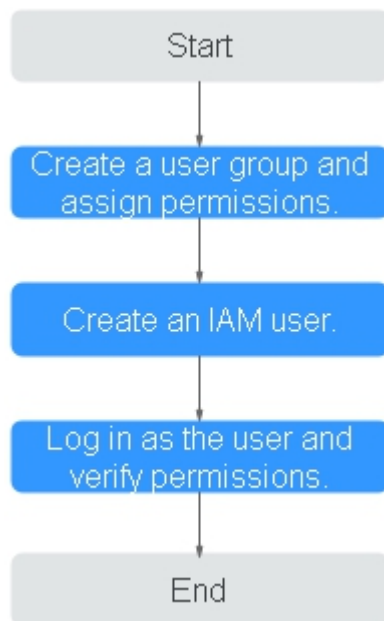
1. On the IAM console, **create a user group and grant it permissions**.

   Create a user group on the IAM console and assign the **CORS ReadOnlyAccess** permissions to the group.

2. **Create an IAM user and add it to the created user group**.

   On the IAM console, create a user and add it to the user group created in **1**.

3. **Log in as the IAM user** and verify the user permissions.

   Log in to the FlexusL instance console as the created user, and verify the read-only permission for the FlexusL instance. (Assume that the user has only the **CORS ReadOnlyAccess** permission.)

   – On the FlexusL instance console, perform other operations except for query operations, for example, purchase a FlexusL instance. If you do not have the permission to purchase an instance, the **CORS ReadOnlyAccess** permission has taken effect.

   – Choose any other service except FlexusL in **Service List**, such as **Virtual Private Cloud**. If a message is displayed indicating insufficient permissions to access the service, the **IMS ReadOnlyAccess** permission has taken effect.

2 Purchasing a FlexusL Instance

Scenarios

This section describes how to purchase a FlexusL instance on the FlexusL instance management console. 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 need to use a private image to create a FlexusL instance, understand **the constraints on private images** of the FlexusL instance in case the image cannot be used after the instance is created.

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. If you want to use a **private image** to create a FlexusL instance, create a private image on the **Image Management Service (IMS)** console. Private images can be used by FlexusL instances only after they are created on the IMS console. For more information, see **Creating a FlexusL Instance from a Private Image or Using a Private Image to Change the OS**.

Procedure

Follow the steps below to purchase a FlexusL instance.

1. Log in to the FlexusL **console** and click **Buy FlexusL**.

2. 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. ● When instances in the regions outside the Chinese mainland access clients in the Chinese mainland across borders, there may be network latency and packet loss.
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 **constraints on private images** 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. Instance specifications include the vCPU/memory, system disk, monthly data package, and peak bandwidth. **NOTE** ● A FlexusL instance is actually a package of different resources. Resources in the package are created, unsubscribed, and renewed together. Resources in the instance specifications cannot be modified, disassociated, or unsubscribed from separately. ● The excess outbound traffic out of the package will be billed by traffic. For details, see **Instance Specifications**.
(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 Services	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 purchase a data disk during the purchase process, you can purchase it afterwards on the FlexusL console.
Required Duration	The minimum duration of a purchase is one month and the maximum duration is three years. Auto-renew can be enabled, which means that 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: Your subscription will be automatically renewed each month. ● Yearly: Your subscription will be automatically renewed each year. For more information about auto-renewal rules, see **Auto-Renewal Rules**.
Quantity	Set the number of FlexusL instances to be purchased.

📖 **NOTE**

A FlexusL instance uses the default network configurations during the creation.

- Public network: By default, a fixed elastic IP address (EIP) is assigned to a FlexusL instance. It cannot be changed.
- Private network: By default, a fixed private IP address 172.31.*x.x*) and VPC (subnet-default-smb) are allocated to a FlexusL instance. They cannot be changed.

  If the network segment of an existing FlexusL instance is 192.168.*x.x*, you need to unsubscribe from the FlexusL instance and delete the VPC (subnet-default-smb) and its associated subnets and security groups. Then, the network segment of the new FlexusL instance is 172.31.*x.x*.

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.

NOTICE

After a FlexusL instance is created using an application image, do not perform operations such as restarting or stopping the instance, or resetting the password before the image with the pre-installed application is up and running. Otherwise, the installation may fail and you cannot log in to the image application dashboard. For details, see **How Do I Check that an Application Image Has Been Up and Running?**

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 by performing **Resetting the Password for a FlexusL Instance** first and then log in to a FlexusL instance by performing **Logging In to a FlexusL Instance Using VNC**.

- 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 a FlexusL 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 Remotely Logging In to a FlexusL Instance

3.1 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 3-1 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 that for logging in to an ECS. **Logging In to a Linux ECS Using an SSH Password > Logging In to a Linux ECS from a Local Windows Server**	

Cloud OS	Local OS	Login Mode	Requirement
	Linux	Use commands. The method is the same as that for logging in to an ECS. **Logging In to a Linux ECS Using an SSH Password > Logging In to a Linux ECS from a Local Linux Server**	
	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	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 3-2 Windows instance login modes

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

Cloud OS	Local OS	Login Mode	Requirement
	macOS	Install a remote connection tool, such as Microsoft Remote Desktop for Mac. The method is the same as that for 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 that for logging in to an ECS. **Remotely Logging In to a Windows ECS (from a Mobile Terminal)**	
	Windows	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 FAQs for troubleshooting. If the fault persists, 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?**

3.2 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 FlexusL server.

If you cannot use the MSTSC or other remote login tools to log in to a cloud server, you can use the VNC login mode. This login mode is mainly used in emergency O&M scenarios for you to view and perform maintenance operations.

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 by performing **Resetting the Password for a FlexusL Instance**.

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**.
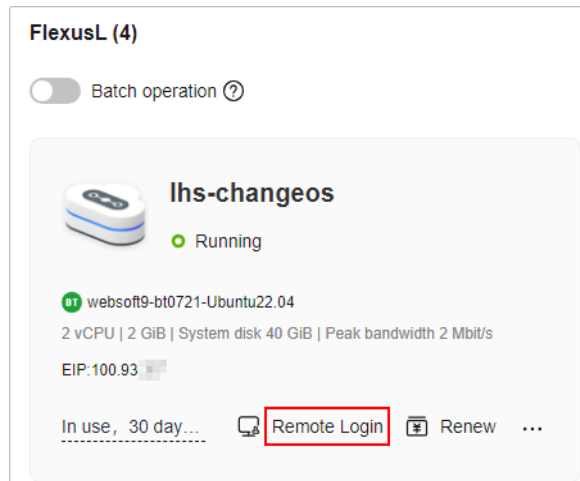
   - Locate the target instance and click 🖥 **Remote Login** in the upper right corner.

   - Locate the target instance, click **Cloud Servers** in the navigation pane on the left, and click 🖥 **Remote Login**.
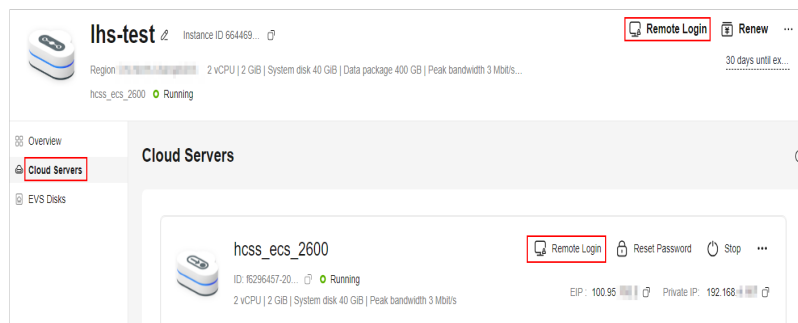
3. Log in to the FlexusL instance following the instructions.

   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**.

3.3 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 3-1 Service authorization
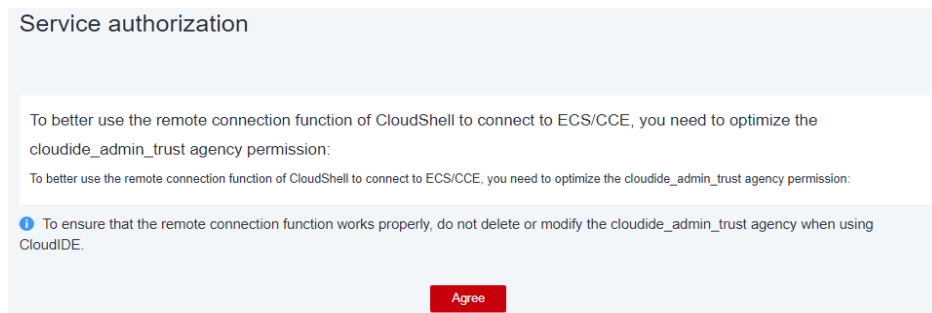
- – If you do not have the Security Administrator permissions, a page will be displayed, requiring you to contact the administrator to assign permissions to you.

  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**.
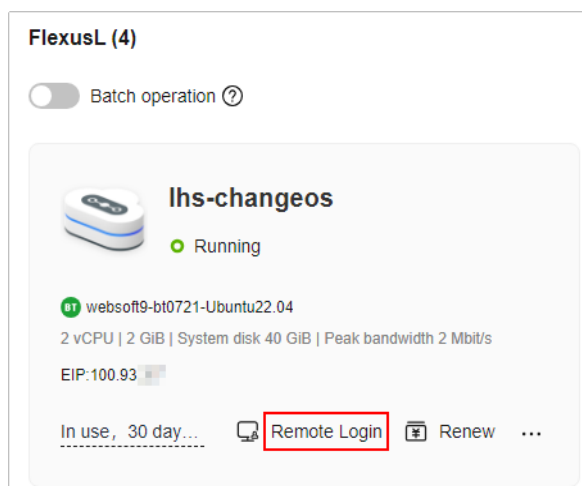
   - – Locate the target instance and click 🖥 **Remote Login** in the upper right corner.
   - – Locate the target instance, click **Cloud Servers** in the navigation pane on the left, and click 🖥 **Remote Login**.
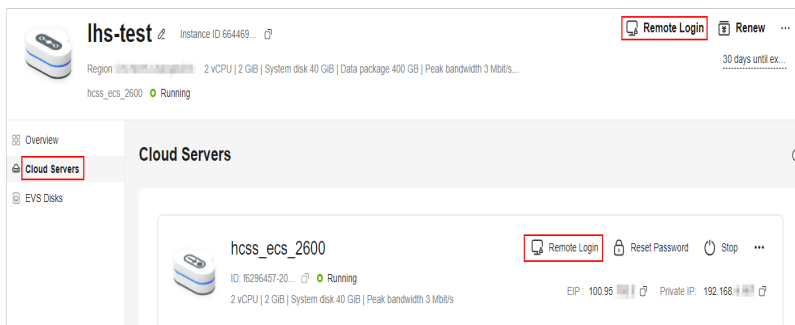
3. In the displayed dialog box, click **Log In via CloudShell** in the **CloudShell Login** area.

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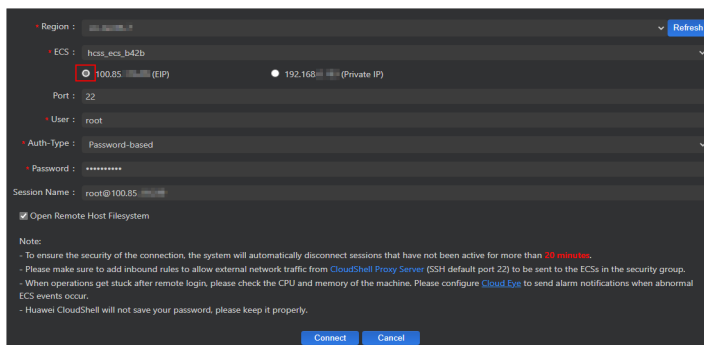
   Table 3-3 Parameters for logging in to the cloud server

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 3-2 Successful login
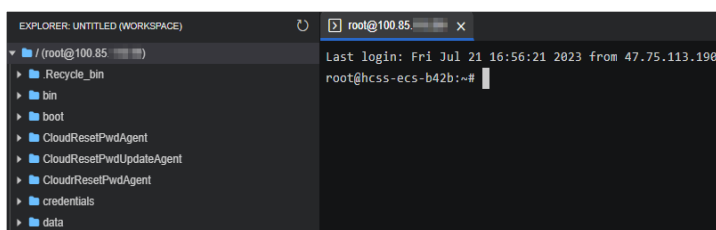
– Using the private IP address

i. Click **Go**.
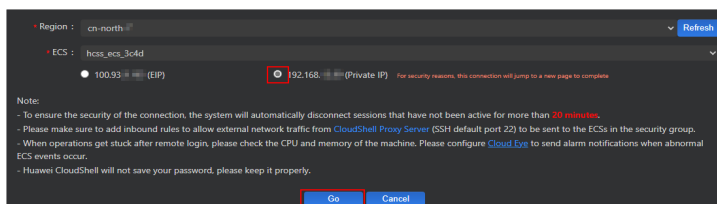
📖 **NOTE**

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 3-3**.

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 by following **Resetting the Password for a FlexusL Instance** and try again.

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

Figure 3-3 Successful login
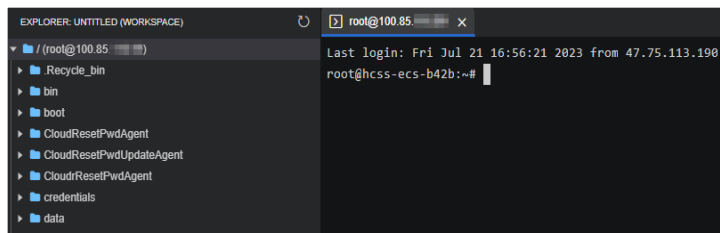
4 Managing FlexusL Instances

4.1 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.
- You have installed the one-click password reset plug-in.

  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:

- Locate the target resource and choose ⋯ > **Reset Password**.

- Click the target instance name. Choose ⋯ > **Reset Password**.

- Click the target instance name. In the navigation pane on the left, choose **Cloud Servers** and click **Reset Password** in the row containing the target server.
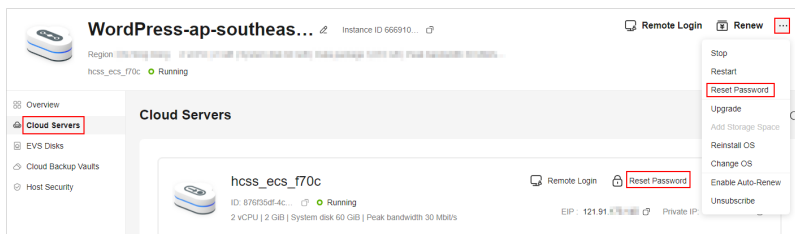
– Batch resetting the login passwords

Enable **Batch operation**, select **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.
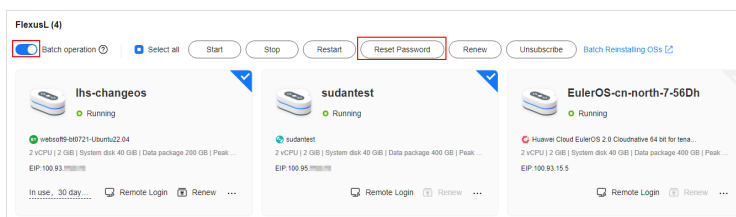
3. Set and confirm a new password as prompted.

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

Figure 4-1 Resetting a password
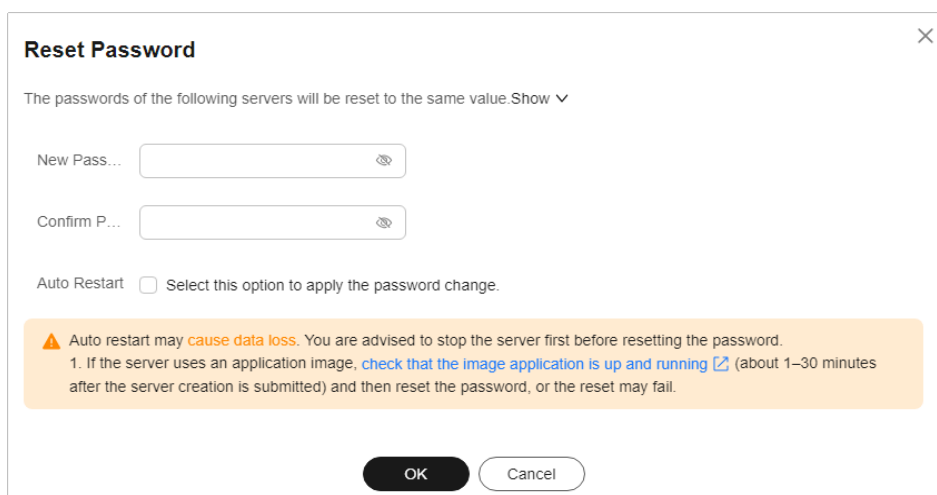
Table 4-1 Password complexity requirements

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.

4.2 Managing OSs of FlexusL Instances

4.2.1 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 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: Click the target FlexusL instance name. On the displayed page, click **Cloud Servers** in the navigation pane on the left and choose ⋯ > **Reinstall OS**.
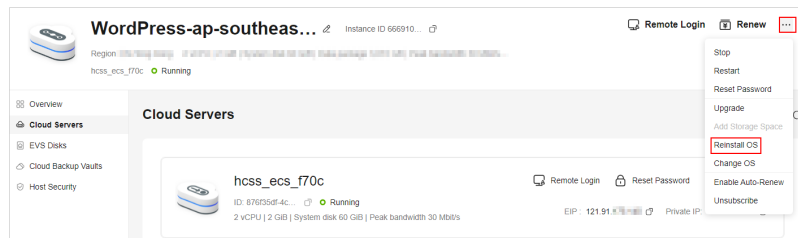
    – Method 3: On the **Cloud Servers** page, click the target server name. In the upper right corner of the details page, choose ⋯ > **Reinstall OS**.

3. Specify the parameters required for reinstalling the OS.

    – Select **Stop server**. The server must be stopped before its OS is 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.

4.2.2 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 OSs are reinstalled, the IP addresses of the cloud servers remain unchanged.

- Reinstalling the OSs clears the data in all partitions, including the system partition, of the system disk. Back up data before reinstalling the OSs.

- Reinstalling the OSs does not affect data disks.

- Do not perform any operations on a cloud server immediately after its OS is reinstalled. Wait for several minutes until the system successfully injects the password, or the injection may fail, and the server cannot be logged in to.

- The servers will automatically restart after the OSs are 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 reinstalling 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 are granted the COC FullAccess permissions, apply for the COC OBT.

3. Synchronize FlexusL instance resources on the **COC console**.

   If you log in to the COC console for the first time, manually synchronize FlexusL instance resources. For details, see **Synchronizing Resources**.

Figure 4-2 Synchronizing FlexusL instance resources
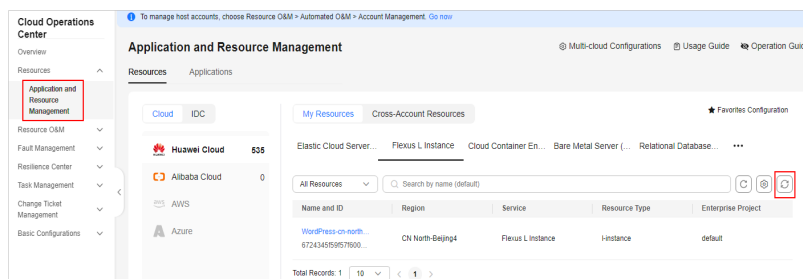
Procedure

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

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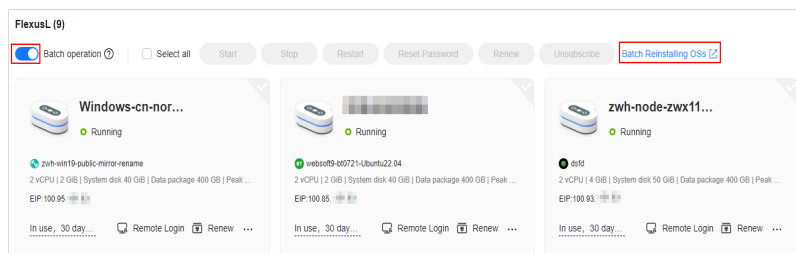
2. On the displayed page, configure parameters required for batch OS reinstallation.

Figure 4-3 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.

Parameter	Description
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 by performing **Resetting the Password for a FlexusL Instance** when logging in to the FlexusL instances for the first time. **NOTE** Currently, FlexusL instances do not support password pairs.

3. 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 page in **Figure 4-4**. 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.
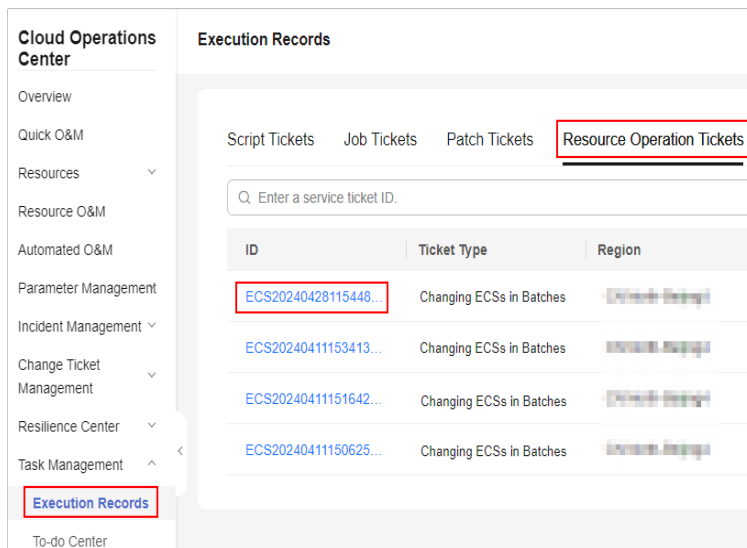
3. In the service ticket details on the displayed page, click **Continue**.

Figure 4-4 Service ticket details
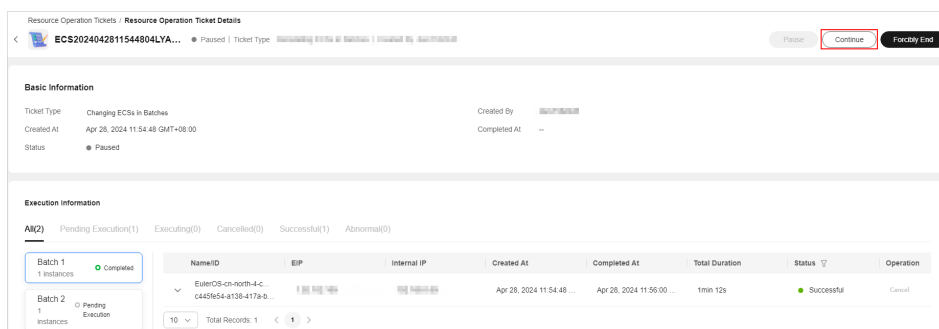
4.2.3 Changing an OS

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 that requires higher specifications. For example, you cannot change the OS of a FlexusL instance with 2 vCPUs and 4 GiB memory using the GitLab application image that needs to use at least 2 vCPUs and 8 GiB memory. To do so, upgrade the FlexusL instance by performing **Modifying the Specifications of a FlexusL Instance** first and try again.

- After the OS is changed, the login password is cleared. You need to reset the password by performing **Resetting the Password for a FlexusL Instance** 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.

- Before using a private image, you need to learn about the constraints on private images in **Table 5-2** for FlexusL instances.

Preparations

If you want to use a private to change the OS of a FlexusL instance, create an image using Huawei Cloud **IMS**. A private image can be used by FlexusL instances only after it is created on the IMS console. For more information, see **Creating a FlexusL Instance from a Private Image or Using a Private Image to Change the OS**.

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.
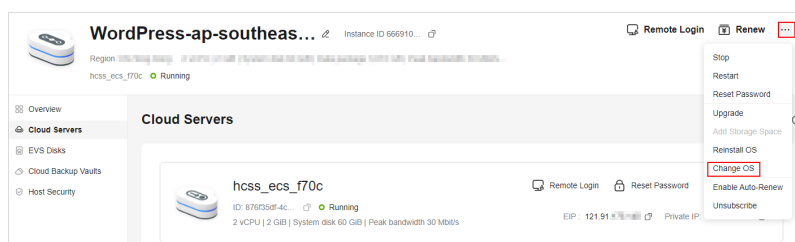
– Method 3: On the **Cloud Servers** page, choose ⋯ > **Change OS** in the row containing the target server.
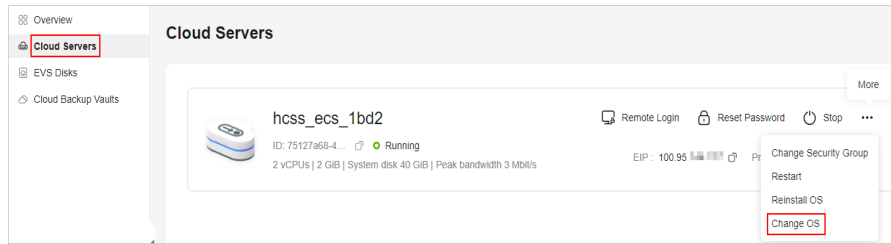
– Method 4: On the **Cloud Servers** page, click the target server name. In the upper right corner of the displayed page, choose ⋯ > **Change OS**.

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, learn about the **constraints on private images** and then create an image. For details, see **Images Supported by FlexusL Instances**.

– Select **Stop server**. The server must be stopped before its OS is changed.
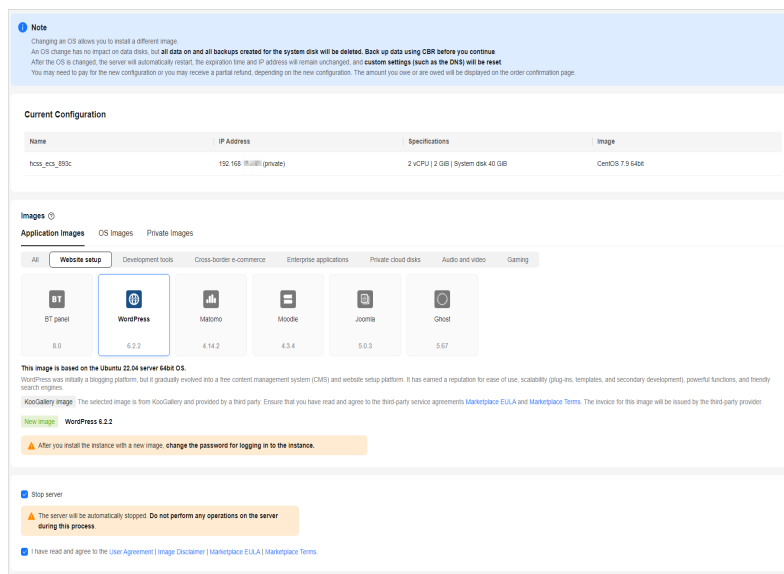
4. Read and agree to the agreements, and click **Submit**.

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 by performing **Resetting the Password for a FlexusL Instance** 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 a FlexusL instance, and the Host Security Service (HSS) is **not protecting** the instance, enable HSS by referring to **What Do I Do If HSS Is Not Started After I Use a Private Image to Create a FlexusL Instance or Change the OS of an Instance?**

4.2.4 Batch Changing OSs of FlexusL Instances

Scenarios

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

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

- FlexusL fixed packages do not support batch OS changes. However, you can change the OS of an individual FlexusL fixed package.
- 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 that requires higher specifications. For example, you cannot change the OS of a FlexusL instance with 2 vCPUs and 4 GiB memory using the GitLab application image that needs to use at least 2 vCPUs and 8 GiB memory. To do so, upgrade the FlexusL instance by performing **Modifying the Specifications of a FlexusL Instance** first and try again.
- After the OS is changed, the login password is cleared. You need to reset the password by performing **Resetting the Password for a FlexusL Instance** 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.
- Before using a private image, learn about the constraints on private images in **Table 5-2** for FlexusL instances.

Preparations

Before batch OS changes, 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 are granted the COC FullAccess permissions, apply for the COC OBT.

3. Synchronize FlexusL instance resources on the **COC console**.

   If you log in to the COC console for the first time, manually synchronize FlexusL instance resources. For details, see **Synchronizing Resources**.

Figure 4-5 Synchronizing FlexusL instance resources
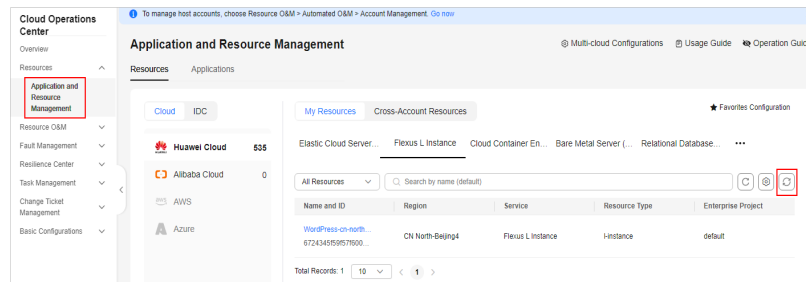
4.   Before using a private image to change the OSs of FlexusL instances, use **IMS** to create an image first. A private image can be used by a FlexusL instance only after it is created using IMS. For more information, see **Creating a FlexusL Instance from a Private Image or Using a Private Image to Change the OS**.

Procedure

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

   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.

   Figure 4-6 Batch changing OSs
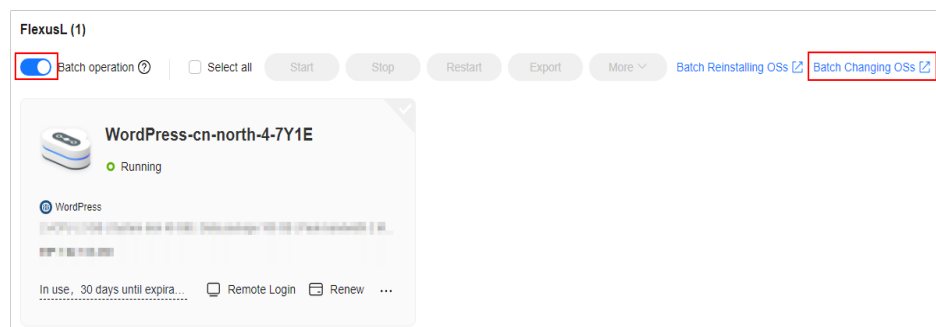
2.   On the displayed page, configure parameters required for batch OS changes.

Figure 4-7 Batch changing 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 changed for FlexusL instances **Region**: Select the region where FlexusL instances are located. The instances must be in the same region. Batch OS change is not available for FlexusL instances in different regions. **Target Instance**: Select the FlexusL instances whose OSs are to be changed. If some FlexusL instances are missing in the list, **synchronize resources first**.

Parameter	Description
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 change 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 changed/Total number of FlexusL instances) x 100%
Stop ECS	This option is displayed when there are FlexusL instances in **Running** state. Select **Stop now**.
Image	Select an image that you want to switch to. FlexusL provides **OS images**, a rich variety of **application images**, and **private images** for you to select. Before using a private image to change the OSs of FlexusL instances, use **IMS** to create an image first. A private image can be used by a FlexusL instance only after it is created using IMS. For more information, see **Creating a FlexusL Instance from a Private Image or Using a Private Image to Change the OS**.

3. Click **Submit**. Confirm the information and click **OK** to start the OS change.

   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.

   After the OS is changed, the cloud server will automatically restart. 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 by performing **Resetting the Password for a FlexusL Instance** 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.

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.

   Figure 4-8 Viewing execution records
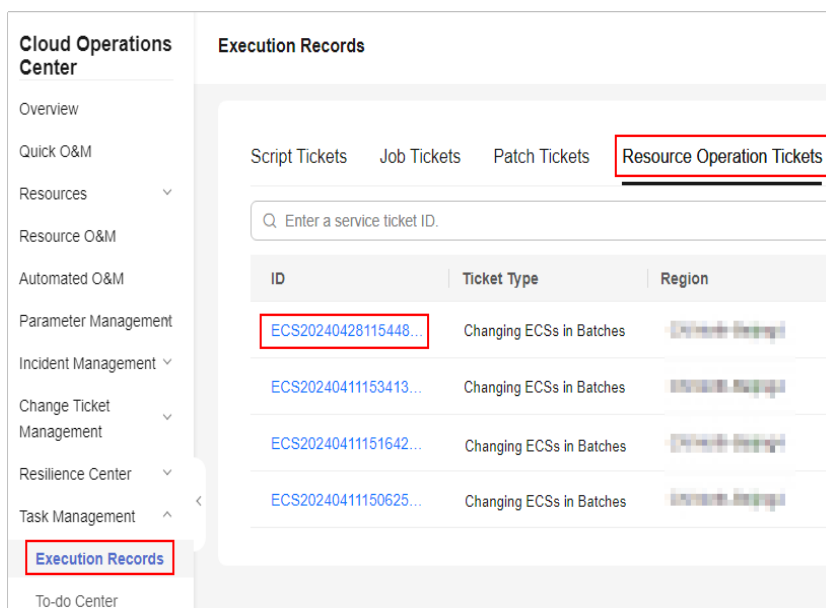
3. In the service ticket details on the displayed page, click **Continue**.

Figure 4-9 Service ticket details
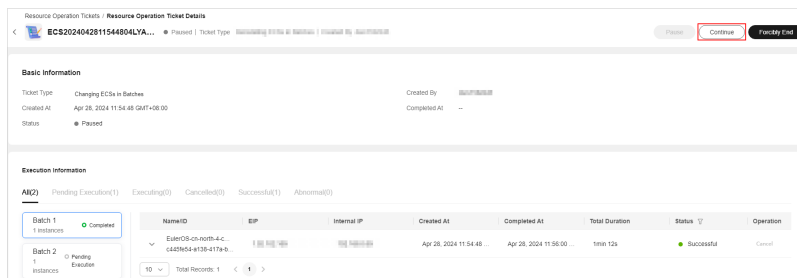
4.3 Modifying the Specifications of a FlexusL Instance

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 new peak bandwidth and data package are lower than the current ones.

Table 4-2 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" > "Specification Upgrades"**.

Preparations

An upgrade failure may result in server data loss. 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. Upgrade the FlexusL instances using any of the following methods:

   – Locate the target FlexusL instance and choose ⋯ > **Upgrade**.
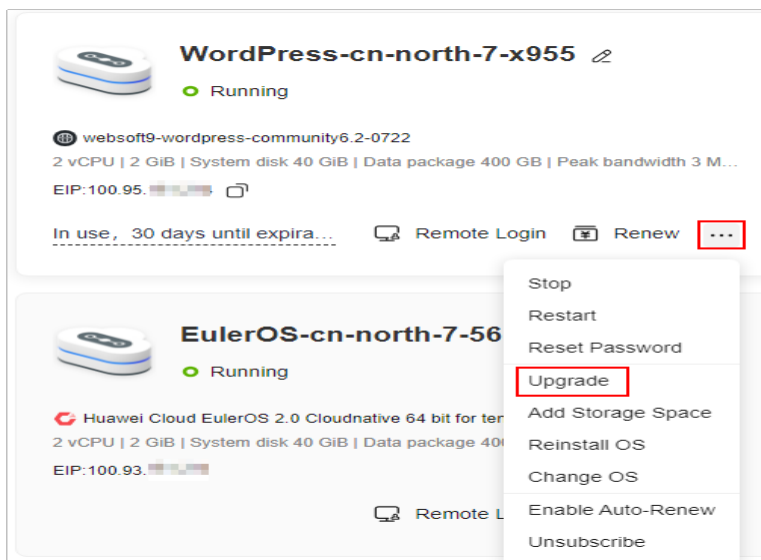
   – On the **Flexus L Instance** page, click the target instance name. On the displayed page, choose ⋯ > **Upgrade** in the upper right corner.
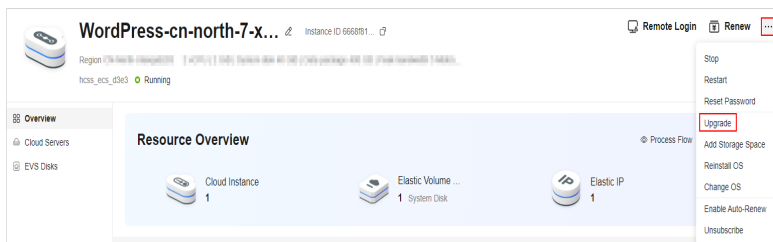
3. Select desired instance specifications on the displayed page.

   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.

4.4 Viewing Information About a FlexusL Instance

4.4.1 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 navigation pane on the left, 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 the following information: ● Basic information: including the instance name, ID, region, and expiration time. ● Configuration information: including the vCPUs/memory, disk capacity and type, bandwidth, and image. ● Network information: including the network interface name and IP address (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**.

Tab	Description
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**.

4.4.2 Searching for a FlexusL Instance

Scenarios

After purchasing a FlexusL instance, you can use the search function on the management console to search for the FlexusL instance 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 4-10 Property and value
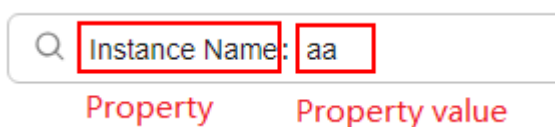
Table 4-3 describes each property.

Table 4-3 Property description

Property	Description
Instance name	Name of a FlexusL instance.

Property	Description
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 4-11** shows the instance ID and cloud server ID on the FlexusL console. **Figure 4-11** 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.

Q EIP : 1.1.1.1 × Add filter

- 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.

Q EIP: 1.1.1.1,1.1.1.2

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.

Q EIP : 1.1.1.1 ×   EIP : 1.1.1.2 ×

- Example 3: Searching by multiple properties with multiple values

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

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

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

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

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

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

Enter at least one date.
Start Date

2024/01/01 00:00:00   🕓

End Date

2024/02/01 00:00:00   🕓

Confirm   Cancel
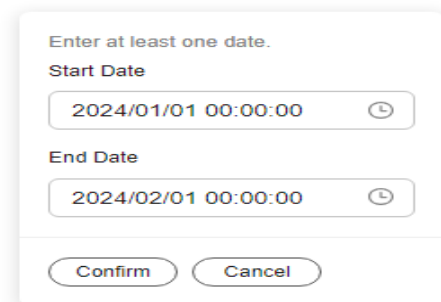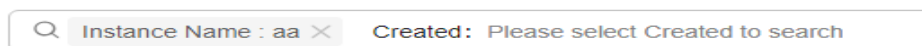
4.4.3 Exporting FlexusL Instance Information

Scenarios

You can export the information of FlexusL instances under your account in an XLSX file to a local directory. This file records the following information about the FlexusL instances: instance names, instance IDs, regions, status, package type, image name, OS type, vCPUs, memory, system disks, data packages, peak bandwidth, cloud server names, cloud server IDs, private IP address, EIP, creation time, and expiration time.

Procedure

1. Log in to the FlexusL **console**.

2. Enable **Batch operation**. Select FlexusL instances to be exported and click **Export**.

   The system automatically exports the information about the selected FlexusL instances to the local PC. In the default download path, view the exported FlexusL instance information.
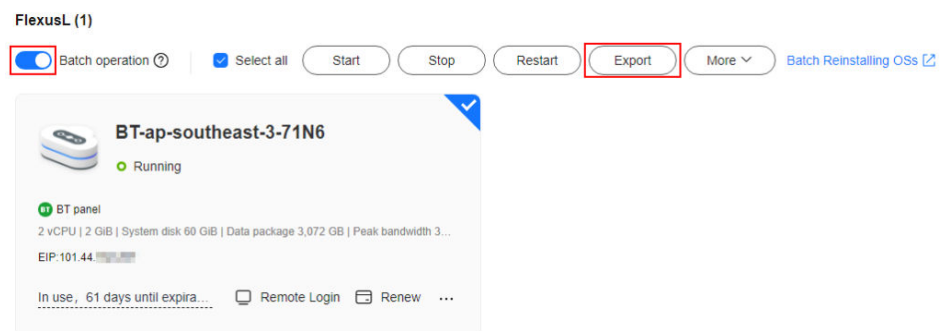
5 Managing Images

5.1 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 how to perform operations on the application image dashboard, see **Logging In to the Application Image Dashboard**.
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 Huawei Cloud or other platforms or downloaded from third party platforms. They can be used by FlexusL only after being created or imported using **Image Management Service (IMS)**.

Image Type	Description
Shared images	A shared image is a private image shared by others. It is a way of using private images flexibly. **NOTE** IMS provides image sharing. You can share private images on the IMS console with other users in the same region.

OS Images

The following table lists the OS images supported by FlexusL.

Image Name	Version	Description
Huawei Cloud EulerOS	2.0	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	7.2/7.3/7.4/7.5/7.6/ 7.7/7.8/7.9/8.0/8.1/ 8.2	CentOS is a popular open-source Linux distribution based on Red Hat Enterprise Linux (RHEL) source code.
Ubuntu	16.04/18.04/20.04/ 22.04	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	9.0/11.1	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 **Logging In to the Application Image Dashboard**.

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.
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.

Image Name	Description
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.
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 asynchronous callback problems, SRS is also cloud native (docker image, Kubernetes 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.

Image Name	Description
EspoCRM	EspoCRM is a web-based customer relationship management (CRM) system designed to help enterprises build and maintain strong customer relationships. It is easy to customize and efficient to use.
KodCloud	KodCloud 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

The following lists the scenarios of FlexusL private images. Shared images are a type of private images and also suitable for to the following scenarios.

- 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) 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)**.

Related Operations

Operation	Description
Logging In to the Image Application Dashboard	You can log in to the visual dashboard of the application image for quick configuration.

Operation	Description
Creating a FlexusL Instance from a Private Image or Using a Private Image to Change the OS	You can use a private image (or a shared image) to quickly create FlexusL instances with the same configurations or change the OS of a FlexusL instance.

5.2 Logging In to the Application Image Dashboard

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 application image dashboard.

Procedure

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 operations. Perform the corresponding operation based on your application. **Table 1** describes how to initialize the application pre-installed in the image.

Table 5-1 Initializing the application pre-installed in the image

Application Image	Initialization
BT panel	**Initialize the BT Panel**
WordPress	**Initialize WordPress**

Application Image	Initialization
Odoo	**Initialize Odoo**
Matomo	**Initialize Matomo**
Portainer	**Initialize Portainer**
GitLab	**Initialize GitLab**
Prestashop	**Initialize Prestashop**
Superset	**Initialize Superset**
Nextcloud	**Initialize Nextcloud**
SRS	Initialization not involved.

Step 2: Logging in to the Application Image 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 application image 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.
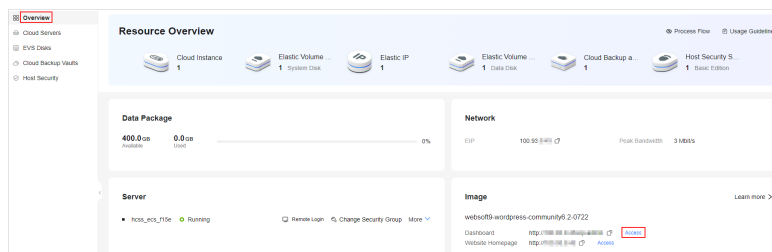
5.3 Creating a FlexusL Instance from a Private Image or Using a Private Image to Change the OS

Scenarios

If you want to use other images except the OS images and application images provided by FlexusL instances, you can create a private image on the **IMS** console. Then, you can use the private image to quickly create a FlexusL instance with the same configurations as the private image or use the private image to change the OS of a Flexus L instance.

Constraints

Table 5-2 Restrictions on private images of FlexusL instances

Item	Description
Region	A FlexusL instance must use a private image that is in the **same region** as the instance, or the image cannot be selected.
Cloud server architecture	Only x86 is supported.
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 Huawei Cloud public Linux images, 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) 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, see **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 create a FlexusL instance or change the OS of a FlexusL instance, create a private image on the **IMS** console. Private images can be used by FlexusL instances only after they are created on the IMS console.

> **NOTICE**
>
> The FlexusL instance and private image must be in the same region, or no private image is available for the FlexusL instance. For example, if you want to create an instance in the CN-Hong Kong region, you can only select images from the CN-Hong Kong region. If you want to use images across regions, replicate the images from other regions to the current region first. For details, see **Replicating Images Across Regions**.

Table 5-3 Creating or sharing an image using IMS

Image Source		Related Operations
Scenario 1	If your private image is created from a Huawei Cloud ECS or BMS, 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: • 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 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

When creating a FlexusL instance or changing the OS of a FlexusL instance, you can click **Private Images** and select a private image from the list. For details about how to create or change the OS of a FlexusL instance, see **Purchasing a FlexusL Instance** and **Changing an OS**.

> 📖 **NOTE**
>
> If the private image is not displayed in the list, check whether the private image is in the same region as the FlexusL instance.
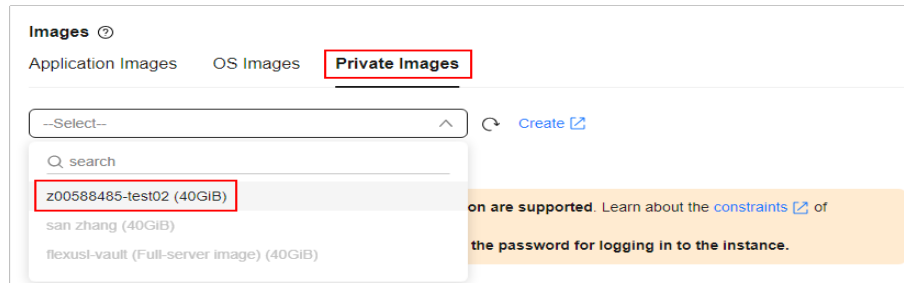
Related Operations

- 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 a FlexusL 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?**

6 Managing EVS Disks

6.1 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 **Modifying the Specifications of 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 ranges from 10 to 2,048, 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 details about 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 can only 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.

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.

Related Operations

Function	Description
Adding a Data Disk	If you have additional storage requirements, you can purchase a data disk on the FlexusL console. Then the system automatically attaches the data disk to the FlexusL instance.
Expanding Capacity of a Data Disk	If the capacity of a data disk cannot meet service requirements, you can expand the capacity of the data disk.

6.2 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 a data disk. You can add a data disk to a cloud server using either of the following methods:

- Method 1: Purchase a data disk on the cloud server console. In this case, the data disk is automatically attached to the cloud server.

- Method 2: Purchase a data disk on the EVS console and manually attach it to a cloud server, or attach an existing EVS disk to a cloud server.

For FlexusL instances, you can only purchase data disks on the FlexusL instance console (method 1). You can purchase a data disk when purchasing a FlexusL instance or after the FlexusL instance is created.

This section describes how to purchase a data disk on the FlexusL instance console after a FlexusL instance is created.

Constraints

- 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.
- A FlexusL instance only supports one data disk. If there is already a data disk, no more data disks can be added.
- 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 Storage Space** 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 details about 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.

6.3 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 **Modifying the Specifications of 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 data 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 details about 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.

ℹ **Note**

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

Expand Data Disk

Current Capacity

50 GiB

New Capacity

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

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

Expiration

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

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

4. Click **Buy Now** and complete the payment as prompted.

   After the purchase, check whether the disk capacity has increased on the console.

Step 2: Extend the Disk Partition and File System

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

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

7 Managing Server Security

7.1 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 7-1 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 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 7-2 lists some high-risk ports. Do not use these ports for your services.

Table 7-2 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**.

7.2 Configuring the Security Group for a FlexusL Instance

7.2.1 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.

By default, FlexusL inbound security group rules only allow instances in the same security group to communicate with each other, and all inbound requests are denied. The outbound security group rules enable all ports and allow all requests to pass through the instances in the security group. Each security group has default rules. For details, see **Table 7-3**. You can also customize security group rules. For details, see **Configuring Security Group Rules for a FlexusL Instance**.

Table 7-3 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.

7.2.2 Configuring Security Group Rules for a FlexusL Instance

Scenarios

A security group consists of inbound and outbound rules. You can add security group rules to allow or deny the traffic to reach and leave the FlexusL instances in the security group.

Security group rules allow or deny network traffic from specific sources over specific protocols or specific ports.

- For details about configuration examples, see **Security Group Examples**.
- For details about how to configure security group rules for FlexusL application images, see **Configuring Security Groups for FlexusL Application Images**.

Precautions

- Before configuring security group rules, you need to plan rules for communications among instances in the security group.
- Define simple security group rules. For details about the constraints on the number of rules in a security group, see **Notes and Constraints**.
- After allowing traffic over a port in a security group rule, ensure that the port is opened in the instance. For details, see **Verifying Security Group Rules**.
- Generally, all FlexusL instances created by the same account in the same region are in the same security group and they can communicate with each other by default.

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. Select **Inbound rules** from the **Security Group** drop-down list and click **Add Rule** on the **Security Groups** tab.

   You can click **+** to add more inbound rules. For details about the parameters, see **Adding a Security Group Rule**.

   Figure 7-1 Adding an inbound rule
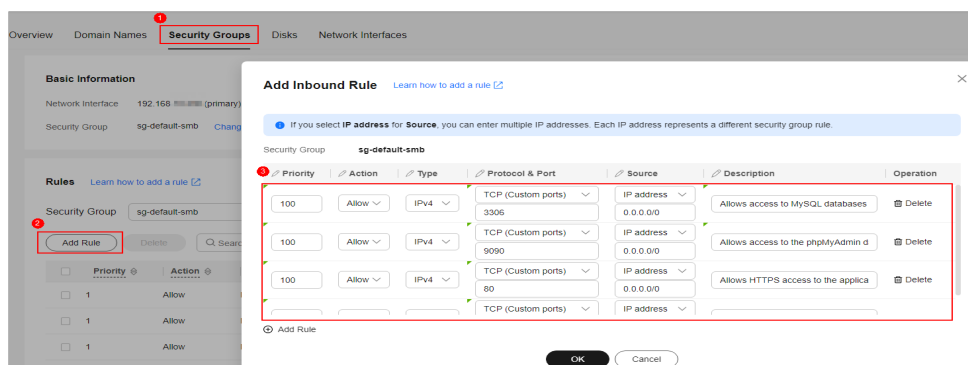
4. Select **Outbound rules** from the **Security Group** drop-down list and click **Add Rule** on the **Security Groups** tab.

   You can click **+** to add more outbound rules. For details about the parameters, see **Adding a Security Group Rule**.

5. Click **OK**.

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.

7.2.3 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. Alternatively, click the **Security Groups** tab and click **Change Security Group** in the **Basic Information** area.
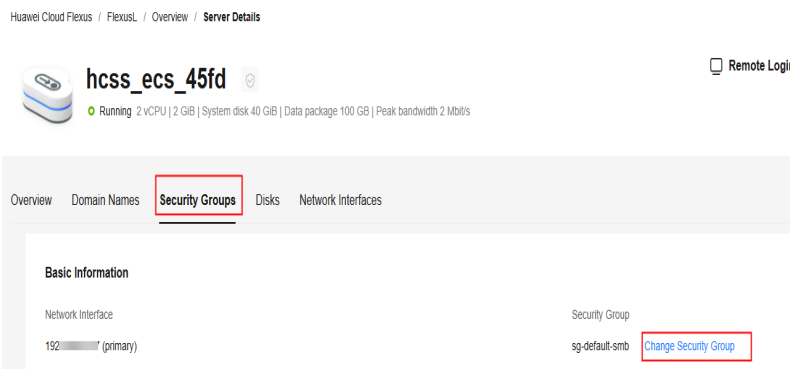
4. Select a security group from the list as needed.

You can select multiple security groups. In this case, the access rules of all the selected security groups apply to 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**.

7.2.4 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 7-4 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 7-5 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 22	0.0.0.0/0	Allows access to the FlexusL instance using SSH locally.
1	Allow	IPv4	TCP: 3306	0.0.0.0/0	Allows access to MySQL databases.
1	Allow	IPv4	TCP: 9090	0.0.0.0/0	Allows access to the phpMyAdmin database management tool.

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 8888	0.0.0.0/0	Allows access to the BT panel dashboard.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows access to the FlexusL instance via HTTPS.
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Allows access to the FlexusL instance via HTTP.

Matomo, Odoo, Nextcloud, and GitLab

Table 7-6 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 page.

Portainer, Superset, and PrestaShop

Table 7-7 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: 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.

Prior ity	Actio n	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M page.

SRS

Table 7-8 Security group rules

Prio rity	Acti on	Typ e	Protoc ol & Port	Sourc e	Description
1	Allo w	IPv4	TCP: 22	0.0.0. 0/0	Allows access to the FlexusL instance using SSH locally.
1	Allo w	IPv4	TCP: 80	0.0.0. 0/0	Specifies the internal forwarding port of application images.
1	Allo w	IPv4	TCP: 9001	0.0.0. 0/0	Allows external access to the application dashboard.
1	Allo w	IPv4	TCP: 1935	0.0.0. 0/0	Allows access to the RTMP livestreaming server.
1	Allo w	IPv4	TCP: 1985	0.0.0. 0/0	Allows access to the HTTP API server to deliver HTTP-API and WebRTC streams.
1	Allo w	IPv4	TCP: 8080	0.0.0. 0/0	Allows access to the HTTP livestreaming server to deliver HTTP-FLV and HLS streams.
1	Allo w	IPv4	TCP: 8000	0.0.0. 0/0	Allows access to the WebRTC media server.

7.3 Configuring HSS for a FlexusL Instance

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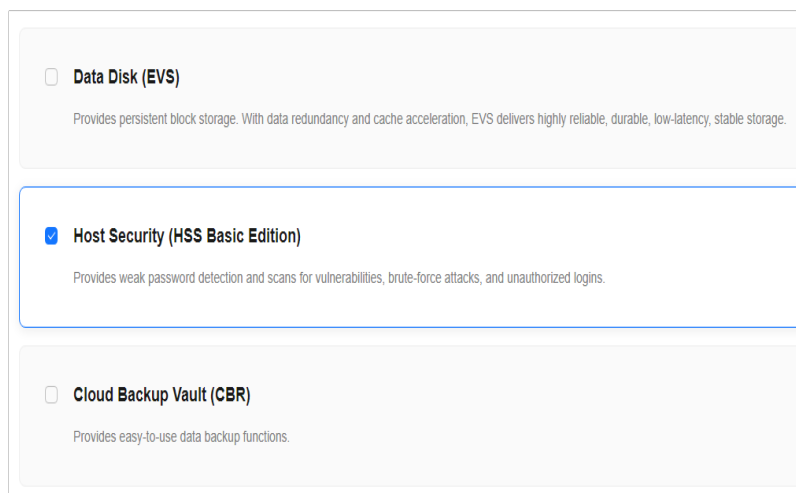
After installing the HSS agent on your instances, you will be able to check the protection status of the instances and risks in a region on the HSS console.

For more information about HSS, see **What Is HSS?**

Enabling HSS

- Scenario 1: Enabling HSS when you purchase a FlexusL instance

  You can associate HSS with your FlexusL instance when you purchase FlexusL on the FlexusL console. The HSS agent will be installed on and HSS will be enabled for the FlexusL instance automatically.

Figure 7-2 Enabling HSS during the purchase of a FlexusL instance

- Scenario 2: Enabling HSS after a FlexusL instance is purchased

  If you do not enable HSS during the FlexusL instance purchase, you can manually install the agent to use HSS. For details, see **Installing the Agent on Servers** and **Enabling Protection**.

  Before manually installing the agent, check whether the OS is supported. For details, see **OS Restrictions**.

The following table lists the differences between enabling HSS in difference scenarios. You can select one as required.

Table 7-9 Differences between two scenarios of HSS

Scenario	Billing Mode	Lifecycle	HSS Version	Advantage
Scenario 1	Yearly/ Monthly (The validity period is the same as that of a FlexusL instance.)	If HSS is enabled during the FlexusL instance purchase on the FlexusL console, its lifecycle is the same as the FlexusL instance. It cannot be renewed or unsubscribed separately, and cannot be disassociated from the FlexusL instance.	Basic Edition	More cost-effective than the yearly/ monthly HSS with the same duration purchased on the HSS console

Scenario	Billing Mode	Lifecycle	HSS Version	Advantage
Scenario 2	Yearly/ monthly and pay-per-use	HSS purchased on the HSS console has its own lifecycle. You can disassociate it from the FlexusL instance at any time.	Basic, enterprise, and premium editions	More flexible

Constraints

If HSS is enabled during the FlexusL instance purchase, it cannot be disassociated after the FlexusL instance is created.

Viewing the Security Status of FlexusL Instances

To view detection details about HSS enabled during the FlexusL instance purchase, perform the following steps. To view detection details about HSS that is not enabled during the FlexusL instance purchase, see **Viewing Detection Details**.

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 **Host Security** to view HSS details.

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

8 Managing Backups

8.1 FlexusL Cloud Backup Overview

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

☐ **NOTE**

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

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 8-1 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 a 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	More cost-effective 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	10–10,485,760, 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.
- Data on FlexusL instances cannot be restored using snapshots.

Related Operations

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

8.2 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.

Preparations

Before backing up a FlexusL instance, ensure that your FlexusL instance has been associated with CBR.

- If you have purchased CBR along with a FlexusL instance, the FlexusL instance is automatically associated with CBR.

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

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 navigation pane on the left and click **Apply Policy** in the upper right corner.
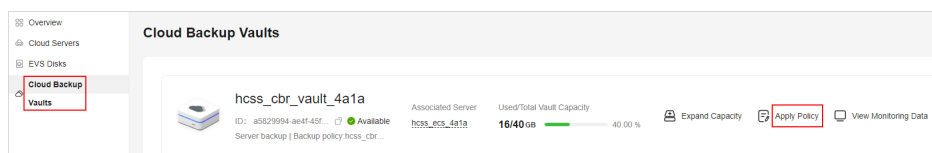
3. View or set the backup policy parameters.

   For details about the parameters, see **Backup policy parameters**.

   📖 **NOTE**

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

4. Click **OK**.

   After creating the backup policy, ensure that the 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 navigation pane on the left on the displayed page to obtain the server name or ID, or vault name or ID.
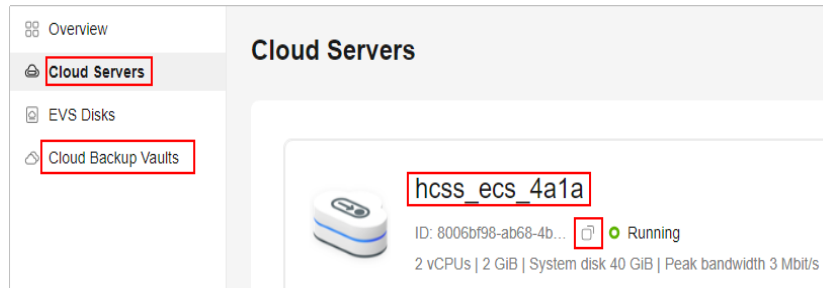
- If you associate a vault with a FlexusL instance server on the CBR console after the FlexusL instance is created, search by server ID.

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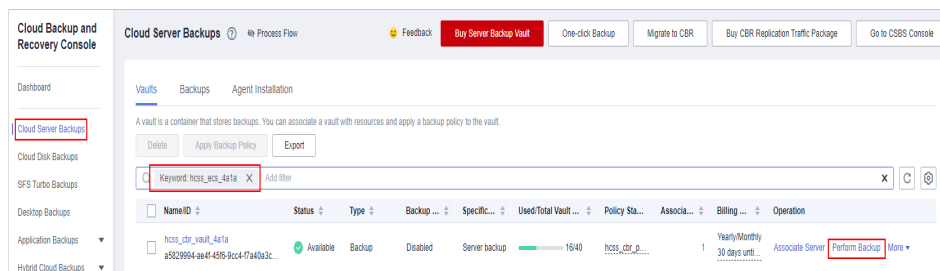
3. Set a backup name and determine whether to enable **Full Backup**.

   Full Backup: If enabled, a full backup task will be performed for the cloud server. If not, an incremental backup task will be performed.
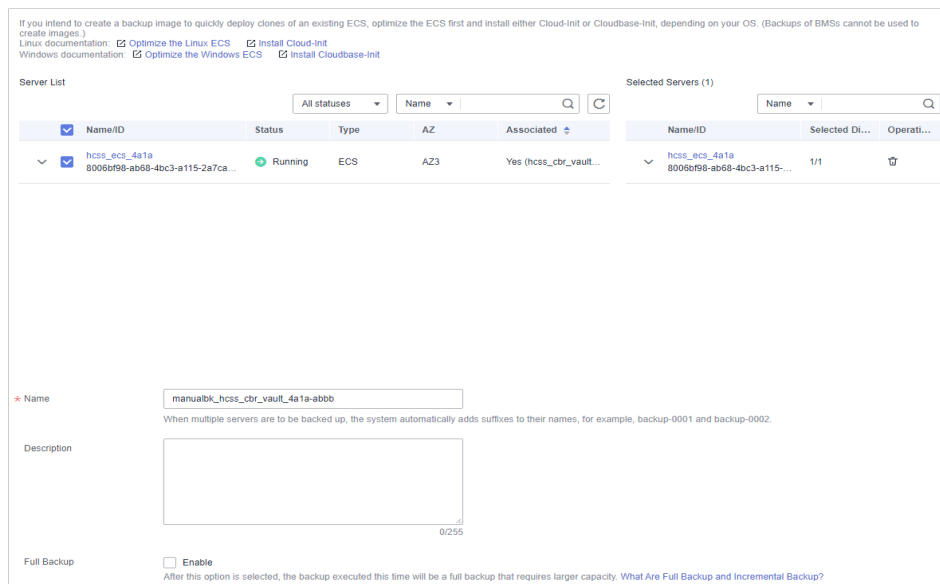
4. Click **OK** to start the backup immediately.

   You can view the created backup on the **Backups** tab page and use the backup to restore data when needed.
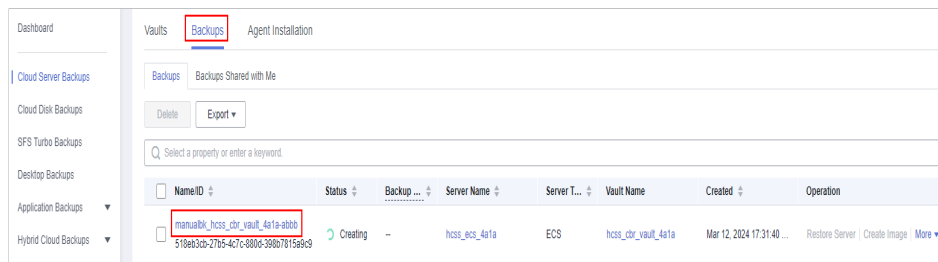
Follow-Up Operations

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**.

8.3 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**.
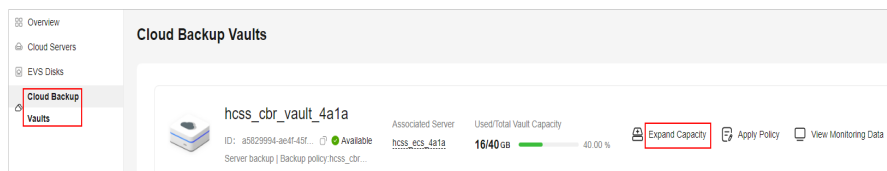
3. On the displayed page, enter a new capacity.

   The vault capacity must be at least as big as the server capacity 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.

9 Managing Domain Names

9.1 Overview

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

Process of Accessing a Website Using a Domain Name

1. Register a domain name.

2. Purchase a FlexusL instance.

3. Apply for ICP licensing for the website and domain name.

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

   📖 **NOTE**

   > Applying for ICP licensing is only allowed when you 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.

9.2 Adding a Domain Name

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

Constraints

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

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

Procedure

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

2. In the navigation pane on the left, choose **Cloud Servers** and then click the server 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 by performing **Resolving a Domain Name**.

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 configured 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.

9.3 Resolving a Domain Name

To enable your website to be accessed using a domain name, you need to configure DNS for it.
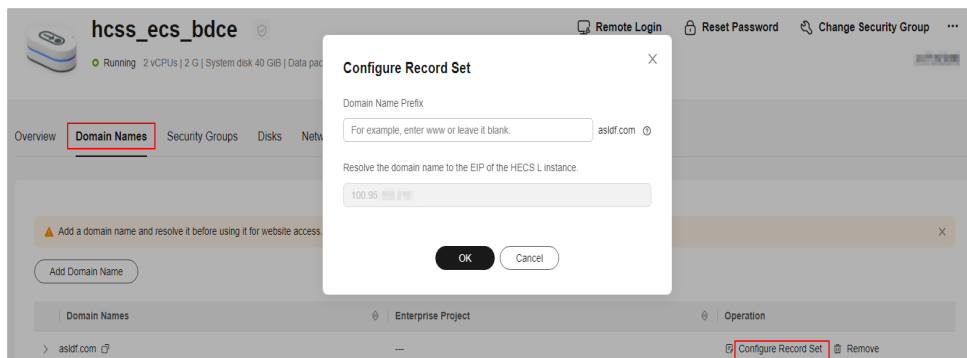
Prerequisites

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 a maximum of 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	Description
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:

   – 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

   For details about how to change the DNS server addresses of a third-party registrar, see **Changing DNS Servers for a Public Domain Name**.

📖 **NOTE**

- If the domain name is registered with Huawei Cloud, skip this step.
- The time required for applying the new DNS server configuration is determined by the DNS service provider.

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_.

10 Monitoring

10.1 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 10-1**.

- 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 10-1 Basic monitoring metrics

Basic Monitoring Metric	Description
CPU Usage	CPU usage of the physical server accommodating the monitored cloud server, which is not as accurate as that obtained from the cloud server that is being monitored Unit: percentage (%) Formula: CPU usage of a cloud server/Number of CPU cores on the cloud server
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/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 outgoing 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 bytes 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.

10.2 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 navigation pane on the left and click **View Monitoring Data**.
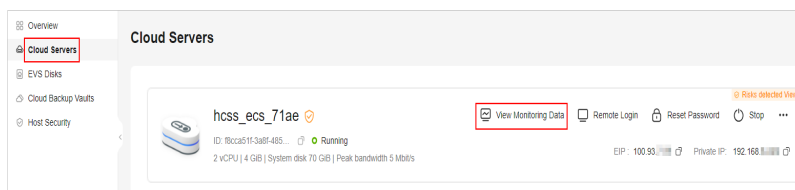
4. View basic monitoring metrics.

   - 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.