Flexus L Instance

User Guide

Issue	01
Date	2025-09-25

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 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.

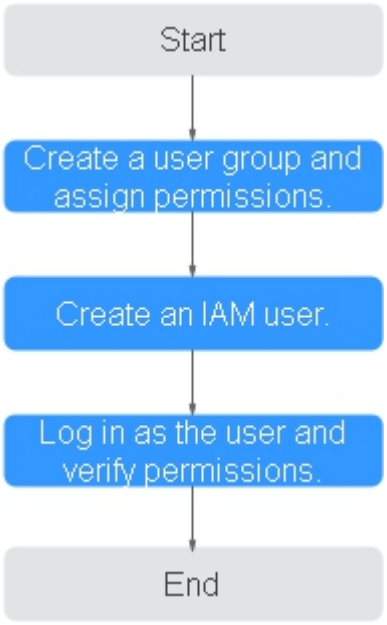
Prerequisites

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 **CORS ReadOnlyAccess** permission has taken effect.

2 Purchasing a FlexusL Instance

Scenarios

This section describes how to purchase a FlexusL instance on the FlexusL console. You can select the region, image, instance specifications, required duration, and other parameters for your FlexusL instances based on your service requirements.

Constraints

- Before purchasing a FlexusL instance, learn about the following constraints. For more details, see **Constraints**.
  - By default, an EIP and a private IP address are assigned to a FlexusL instance. The EIP cannot be changed and will not be retained after the instance is released.
  - The VPC cannot be changed after a FlexusL instance is created.
  - FlexusL instances do not support IPv6 addresses.
  - A FlexusL instance is actually a package of resources. Resources in the package are unsubscribed and renewed together. The EVS disk, backup vault, HSS, and data package included in the package cannot be unsubscribed separately.
  - After a FlexusL instance is purchased, its region cannot be changed. Exercise caution when selecting a region.
- 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 for a HUAWEI ID and Enabling Huawei Cloud Services**.

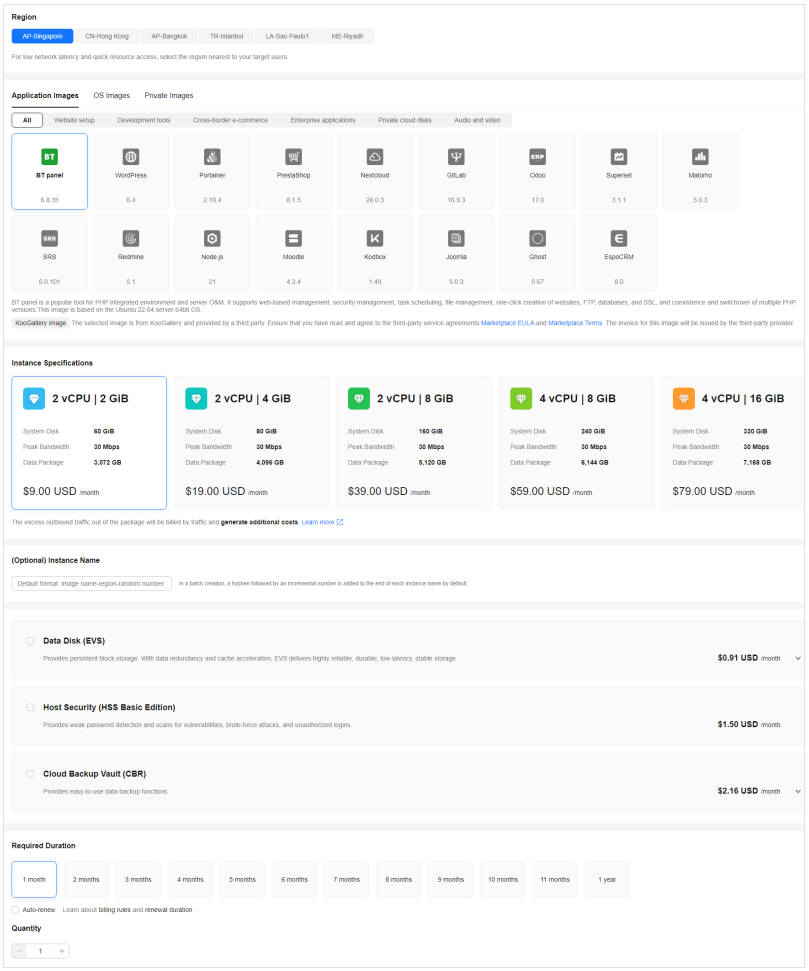
   Real-name authentication is required only when you buy or use cloud services provisioned in the Chinese mainland.
2. If you want to use a **private image** to create a FlexusL instance, create a private image on the **Image Management Service (IMS)** console. Private images can be used by FlexusL instances 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, its 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. For more network information, see **How Does FlexusL Instances Communicate with Each Other and with Other Cloud Resources Over a Private Network?** • When instances in the regions outside the Chinese mainland access instances in the Chinese mainland, there may be network latency and packet loss.
Image	FlexusL provides **OS images**, **application images**, and **private images** for you to select from. Before using a private image, you need to learn about the **constraints on private images** and create the private image. For details, see **Images Supported by FlexusL Instances**.
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 resources. Resources in the package are created, renewed, and unsubscribed from together. Resources in the instance specifications cannot be modified, disassociated, or unsubscribed from separately. • The outbound data usage beyond 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.

Parameter	Description
(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, you can purchase it afterwards on the FlexusL console. For details, see **Overview**. • If you have not purchased HSS at this time, you can purchase and enable it on the HSS console later. For details, see **Configuring HSS for a FlexusL Instance**. • If you have not purchased CBR at this time, you can purchase cloud server backups on the CBR console to back up the FlexusL instance. For details, see **FlexusL Cloud Backup Overview**.
Required Duration	The minimum duration of a purchase is one month and the maximum duration is three years. Auto renewal is supported. It means that 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 after the instances are created. • Monthly: auto-renews for 1 month every time. • Yearly: auto-renews for 1 year every time. 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) and VPC (vpc-default-smb) are assigned to a FlexusL instance. They cannot be changed.
- Private network: By default, a fixed private IP address (172.31.*x.x*) and subnet (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 and its associated subnets and security groups. Then, the network segment of the new FlexusL instance is 172.31.*x.x*.

3. Click **Next: Confirm**.

   On the displayed page, confirm the order details, agree to 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.

> **NOTE**
>
> If you create a FlexusL instance using an application image, it takes some time for the application preinstalled in the image is up and running. During this period of time, do not perform operations such as restarting or stopping the instance, or resetting the password. Otherwise, the installation may fail and you cannot log in to the image application dashboard. 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 the password** first.
- FlexusL instances support multiple login modes. For details, see **Login Modes**.

  Before logging in to a FlexusL instance in non-VNC mode, ensure that the login port is opened in the security group. Otherwise, the cloud server cannot be connected. For example, to log in to a Linux instance, ensure that SSH (22) is opened. To log in to a Windows instance, ensure that RDP (3389) is opened. For details about how to configure security group rules, see **Configuring Security Group Rules for a FlexusL Instance**.
- If you have purchased a data disk, you need to **initialize the data disk** before using it.
- If you select an application image when creating a FlexusL instance, you can log in to the visual dashboard of the image application to quickly configure the application. 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. For details, see **Creating an Nginx Server Using the CentOS Image** or **Setting Up Websites**.

  > **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. Otherwise, the command execution may fail due to 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 image provider, 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 FlexusL 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 FlexusL Instance and I Know the Initial Password of the Private Image?**
- If you use a private image to create a FlexusL instance with Host Security (HSS) included, HSS will not protect the instance. You need to 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?**

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 to connect to the FlexusL instance. For details, see the following: • **Logging In to the Linux Instance from a Local Windows Server** • **Logging In to the Linux Instance from a Local Windows Server**	

Cloud OS	Local OS	Login Mode	Requirement
	Linux	Use commands to connect to the FlexusL instance. For details, see the following: • **Logging In to the Linux Instance from a Local Linux Server** • **Logging In to the Linux Instance 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.

Cloud OS	Local OS	Login Mode	Requirement
	Linux	Install a remote connection tool, such as rdesktop. The method is the same as logging in to an ECS. **Remotely Logging In to a Windows ECS (from a Linux Computer)**	
	macOS	Install a remote connection tool, such as Microsoft Remote Desktop for Mac. The method is the same as 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.

Reference

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

3.2 Logging In to a Linux FlexusL Instance Using CloudShell

Scenarios

CloudShell is an online interactive terminal service available on the Huawei Cloud console. It allows you to access and manage Huawei Cloud resources using a

browser without installing local tools. When you use CloudShell, CloudShell communicates with your cloud servers through the CloudShell proxy IP address. Your real IP address will be hidden to improve your privacy and cloud server security.

This section describes how to log in to a FlexusL instance using CloudShell.

Prerequisites

- The status of the FlexusL instance must be **Running**.
- You have obtained the password for logging in to the cloud server. A FlexusL instance does not have an initial password. If you log in to a FlexusL instance for the first time or forget the password, obtain the password by referring to **Resetting the Password for a FlexusL Instance**.
- Ensure that the external traffic from the CloudShell proxy server (SSH default port: 22) is allowed in the security group. Otherwise, the cloud server cannot be connected. The CloudShell proxy IP address varies depending on the region. The actual proxy IP address will be displayed on the CloudShell configuration page. For details about how to configure security group rules, see **Configuring Security Group Rules for a FlexusL Instance**.

  If you want to use other ports, log in to the cloud server and change the port number. For details, see **How Can I Change a Remote Login Port?**
- 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 (or users with admin permissions) 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 a User Group**.

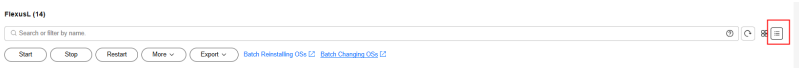
> **NOTE**
>
> When you use CloudShell to remotely connect to an ECS through a public network, service authorization is not required.

Procedure

1. Log in to the FlexusL **console**.
2. Log in to a cloud server using any of the following methods:

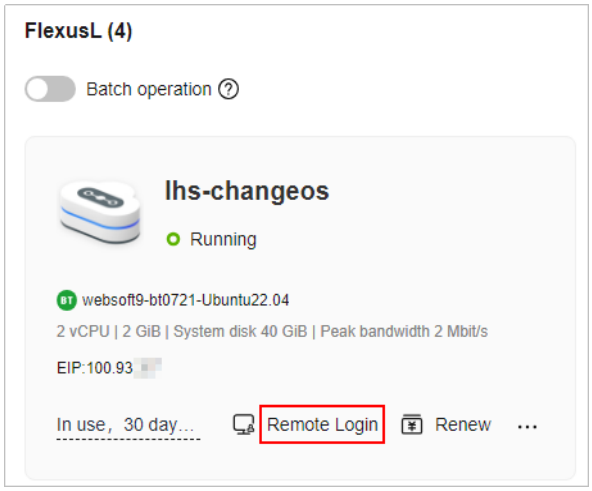
   > **NOTE**
   >
   > By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

   Figure 3-2 Switching views

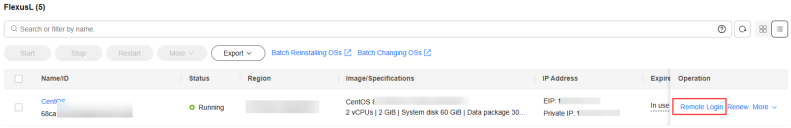
   - Method 1: In the card view, click **Remote Login** on the resource card.

     Figure 3-3 Remote login entry from the resource card

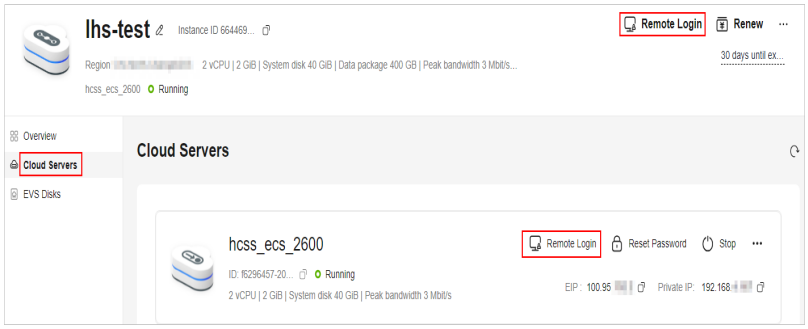
   - Method 2: In the list view, click **Remote Login** in the **Operation** column of the FlexusL instance.

     Figure 3-4 Remote login entry from the list page

   - Method 3: Click the target resource card or instance name. On the displayed page, choose **Cloud Servers** from the left navigation pane and click **Remote Login**.

Figure 3-5 Remote login entry from the cloud server details page



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.

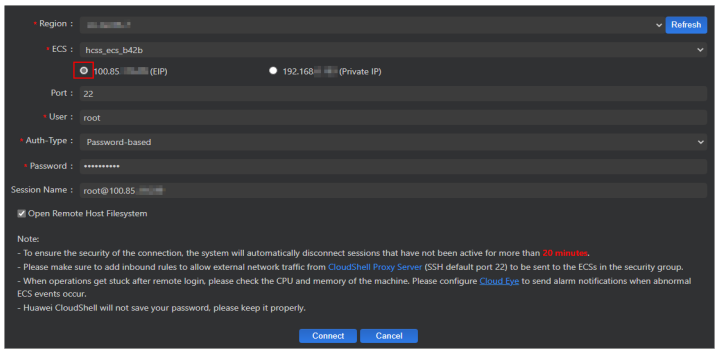


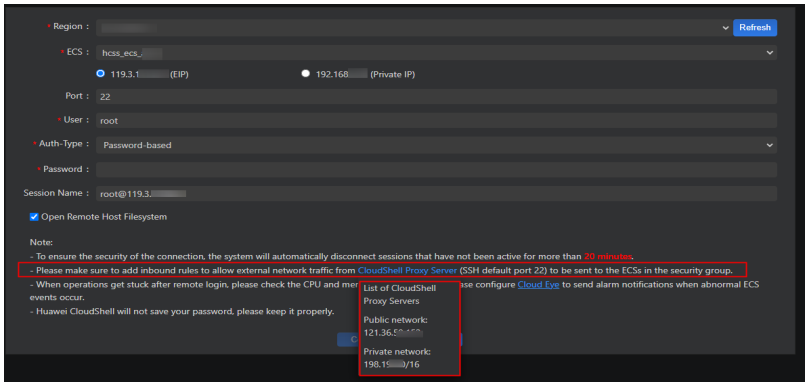
Table 3-3 Parameters for logging in to the cloud server

Parameter	Description
Port	Connection port, which is **22** by default.
User	Username for logging in to the cloud server, which is **root** by default.
Auth-Type	Select **Password-based** and enter the password for logging in to the cloud server. If you have not set the password or forgot the password, **reset it**.
Session Name	The default format is *Username@IP address*. You can change it as needed.

Ensure that the external traffic from the CloudShell proxy server (SSH default port: 22) is allowed in the security group. When you use CloudShell to connect to a cloud server, the CloudShell proxy IP address replaces your actual IP address to send the connection request. You need to add a rule to the security group of the cloud server to allow the traffic from the CloudShell proxy server (port 22). The CloudShell connection will fail if your security group rule only allows your actual IP address to pass through port 22 but blocks the CloudShell proxy IP address. For details about how to configure security group rules, see **Configuring Security Group Rules for a FlexusL Instance**.

The CloudShell proxy IP address may vary depending on the region. The following figure is an example.

Figure 3-6 CloudShell proxy IP address

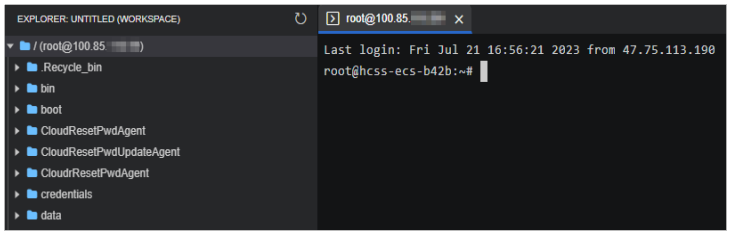


ii. Click **Connect**.

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.

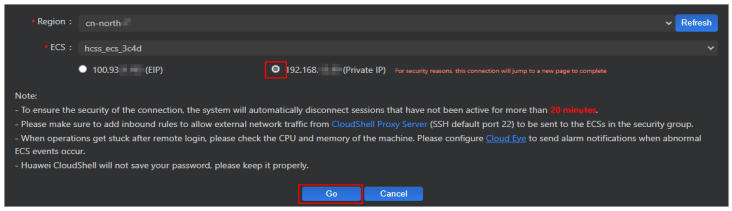
After the connection is successful, a figure similar to the following is displayed:

Figure 3-7 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.

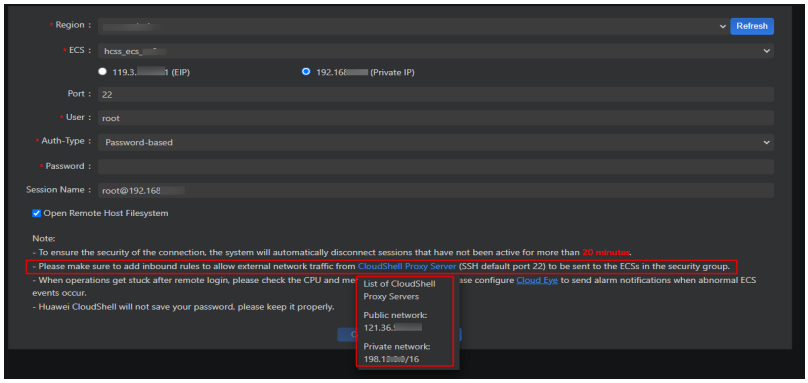
Table 3-4 Parameters for logging in to the cloud server

Parameter	Description
Port	Connection port, which is **22** by default.
User	Username for logging in to the cloud server, which is **root** by default.
Auth-Type	Select **Password-based** and enter the password for logging in to the cloud server. If you have not set the password or forgot the password, **reset it**.
Session Name	The default format is *Username@IP address*. You can change it as needed.

Ensure that the external traffic from the CloudShell proxy server (SSH default port: 22) is allowed in the security group. When you use CloudShell to connect to a cloud server, the CloudShell proxy IP address replaces your actual IP address to send the connection request. You need to add a rule to the security group of the cloud server to allow the traffic from the CloudShell proxy server (port 22). The CloudShell connection will fail if your security group rule only allows your actual IP address to pass through port 22 but blocks the CloudShell proxy IP address. For details about how to configure security group rules, see **Configuring Security Group Rules for a FlexusL Instance**.

The CloudShell proxy IP address may vary depending on the region. The following figure is an example.

Figure 3-8 CloudShell proxy IP address

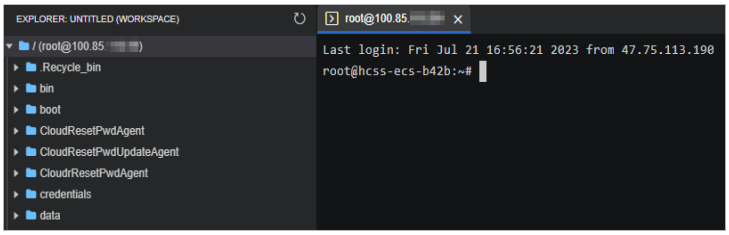


iii. Click **Connect**.

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 3-9 Successful login



Reference

- After login, if you need to use the copy-and-paste function provided by CloudShell, see **Common CloudShell Operations**.
- **What Can I Do If I Forget the Login Password of a FlexusL Instance?**
- **Where Can I Find the Username and Password for Remotely Logging In to a FlexusL Instance?**

3.3 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**.

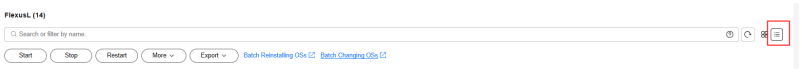
Procedure

1. Log in to the FlexusL **console**.
2. Log in to a cloud server using any of the following methods:

NOTE

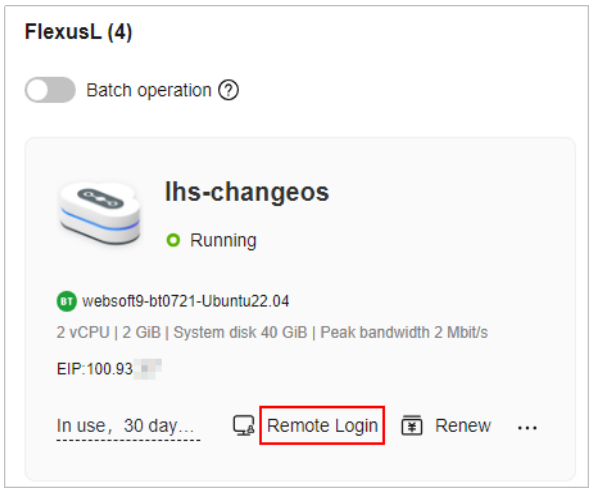
By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

Figure 3-10 Switching views



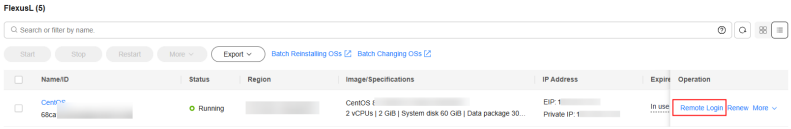
- Method 1: In the card view, click **Remote Login** on the resource card.

Figure 3-11 Remote login entry from the resource card



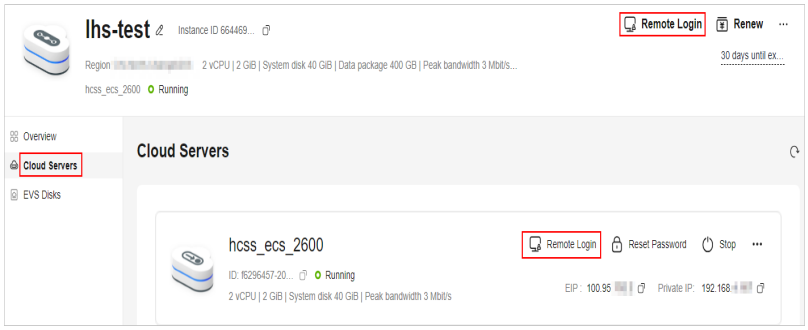
- Method 2: In the list view, click **Remote Login** in the **Operation** column of the FlexusL instance.

Figure 3-12 Remote login entry from the list page



- Method 3: Click the target resource card or instance name. On the displayed page, choose **Cloud Servers** from the left navigation pane and click **Remote Login**.

Figure 3-13 Remote login entry from the cloud server details page

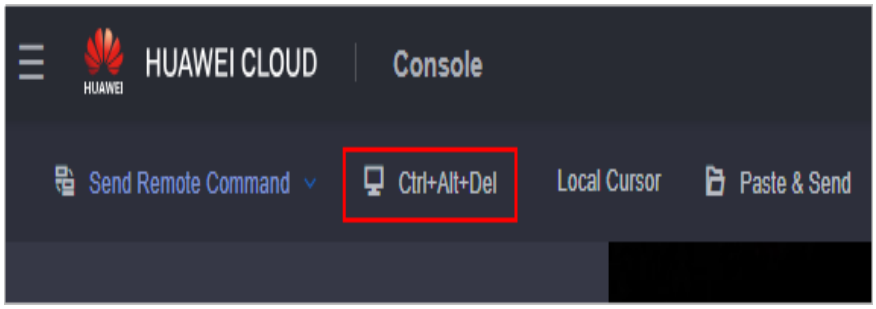


3. Log in to the FlexusL instance following the instructions.

   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.

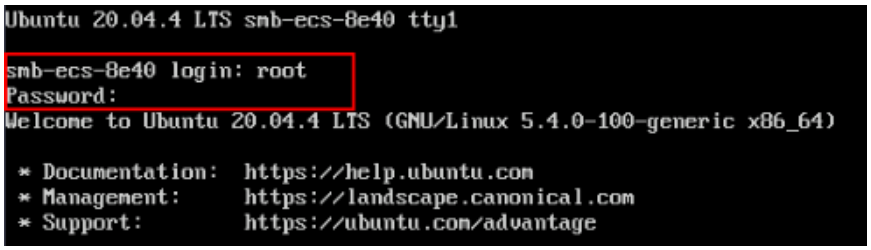
   - For Windows: Click **Ctrl+Alt+Del** to unlock the desktop and enter the password.

     The default username is **Administrator**.

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

     The default username is **root**.

Helpful Links

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

3.4 Logging In to a Linux FlexusL Instance Using an SSH Key Pair

Scenarios

This section describes how to remotely log in to a Linux instance using an SSH key pair in Windows and Linux.

Prerequisites

- You have created or imported a key pair. For details, see **Creating a Key Pair** and **Importing a Private Key**.
- You have bound the key pair to the instance to be logged in to. For details, see **Binding a Key Pair to an ECS**.

Search for the FlexusL instance in the cloud server list on the DEW console using its server name or ID. On the FlexusL console, click the target instance. On the Cloud Servers page, you can view the cloud server name and ID.

Figure 3-14 Viewing the server name and ID of a FlexusL instance

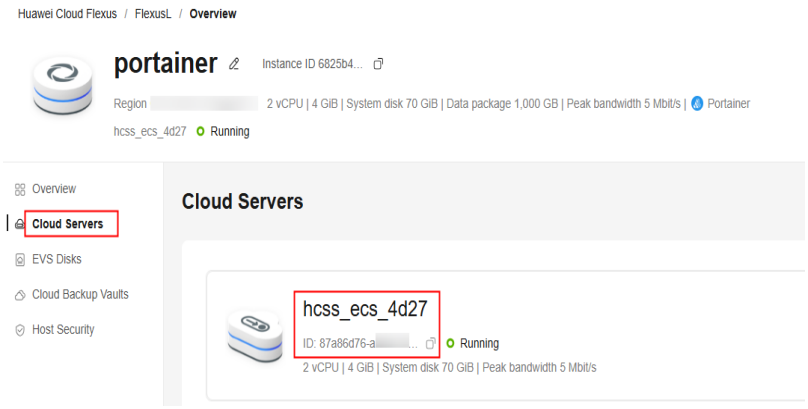
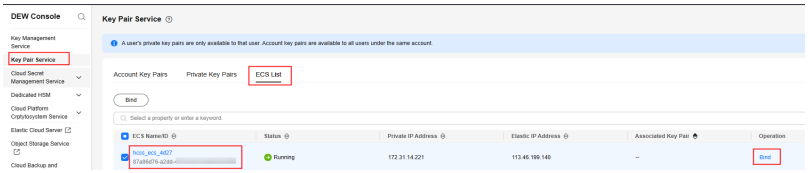


Figure 3-15 Binding a key pair to a FlexusL instance



- Port 22 is allowed in the inbound direction of the security group to which the cloud server belongs. For details, see **Configuring Security Group Rules for a FlexusL Instance**.
- The network connection between the login tool (PuTTY) and the target cloud server is normal. For example, the default port 22 is not blocked by the firewall.

Logging In to the Linux Instance from a Local Windows Server

You have two methods to log in to a Linux instance from a local Windows server.

Method 1: Use PuTTY to log in to the instance.

The following operations use PuTTY as an example. Before using PuTTY to log in, make sure that the private key file has been converted to .ppk format.

1. Check whether the private key file has been converted to .ppk format.
   - If yes, go to step **7**.
   - If no, go to step **2**.
2. Visit the following website and download PuTTY and PuTTYgen:
   https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

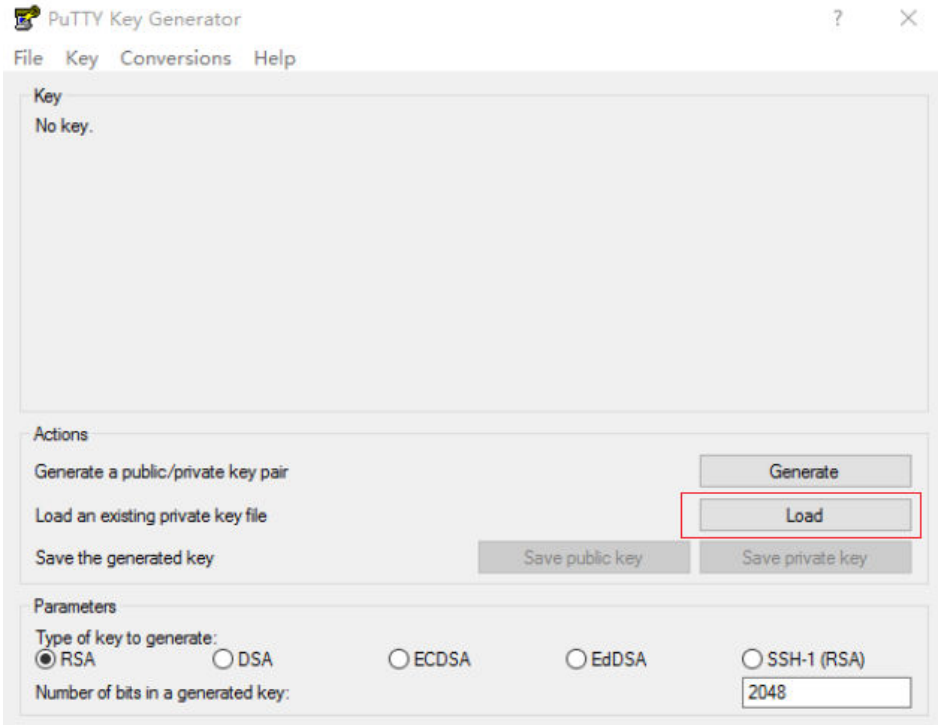
   NOTE

   PuTTYgen is a private key generator, which is used to create a key pair that consists of a public key and a private key for PuTTY.
3. Run PuTTYgen.

4. In the **Actions** pane, click **Load** and import the private key file that you stored during instance creation.

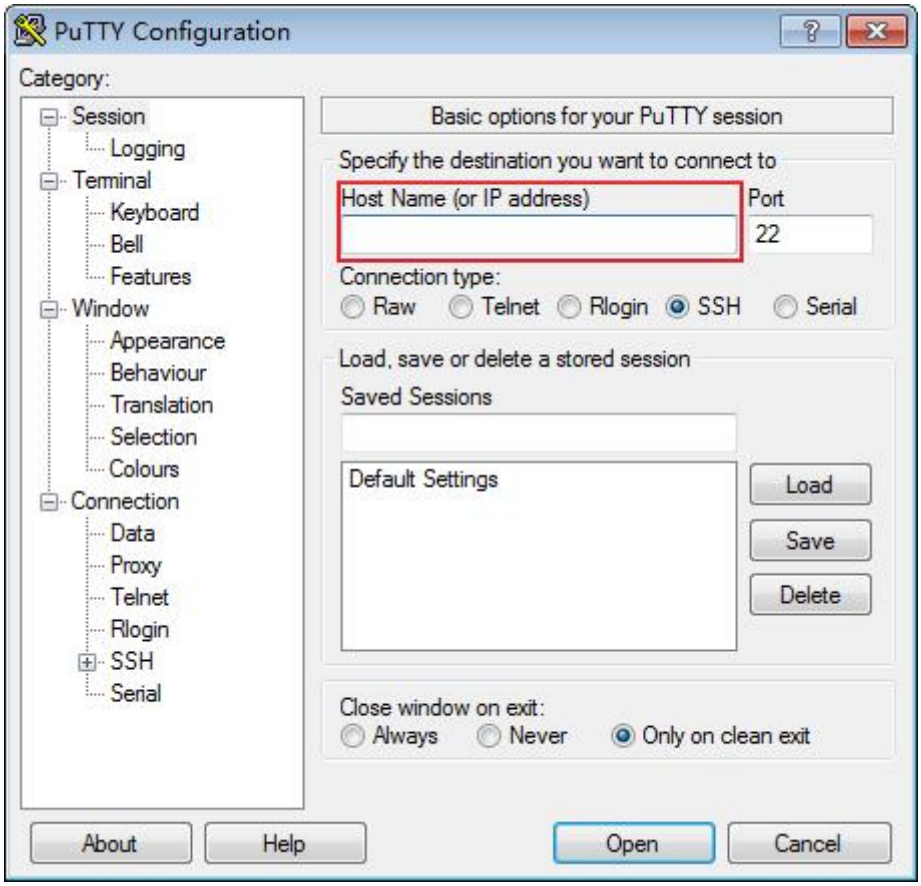
   Ensure that the format of **All files (*.*)** is selected.

   Figure 3-16 Importing the private key file



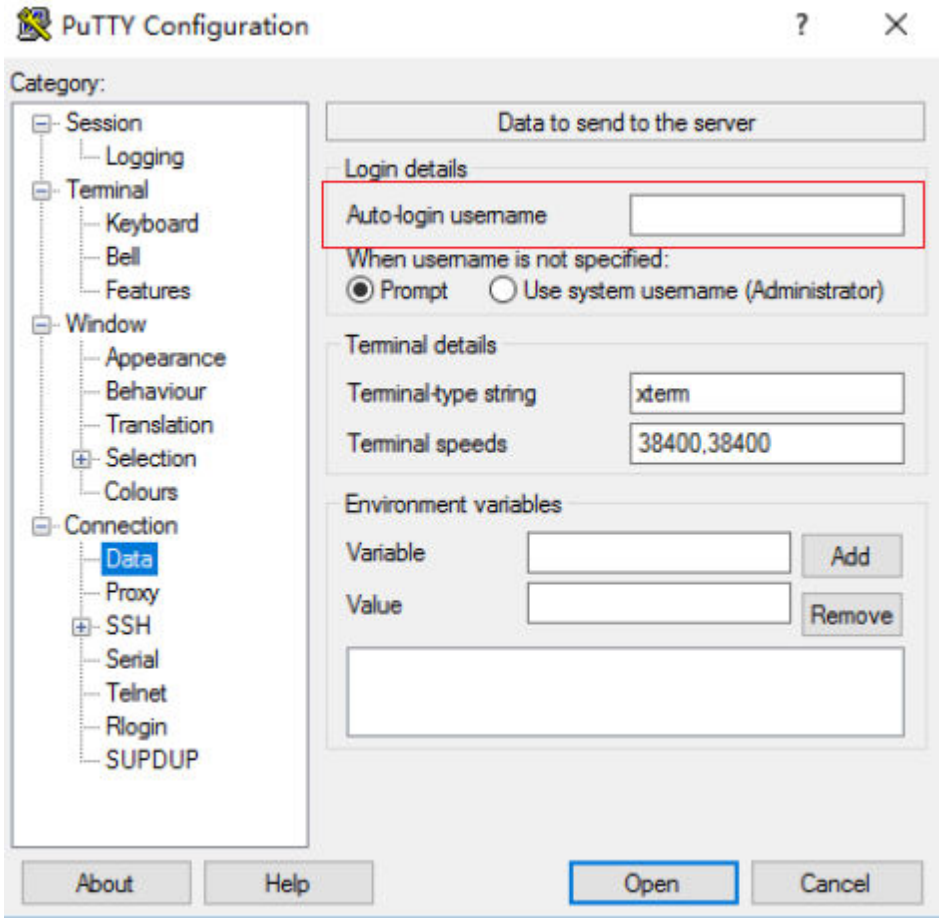
5. In the **Actions** area, click **Save private key**.
6. Save the converted private key, for example, **kp-123.ppk**, in a local directory.
7. Double-click **PUTTY.EXE**. The **PuTTY Configuration** page is displayed.
8. Click **Session** and enter the elastic IP address bound to the cloud server under **Host Name (or IP address)**.

Figure 3-17 Configuration



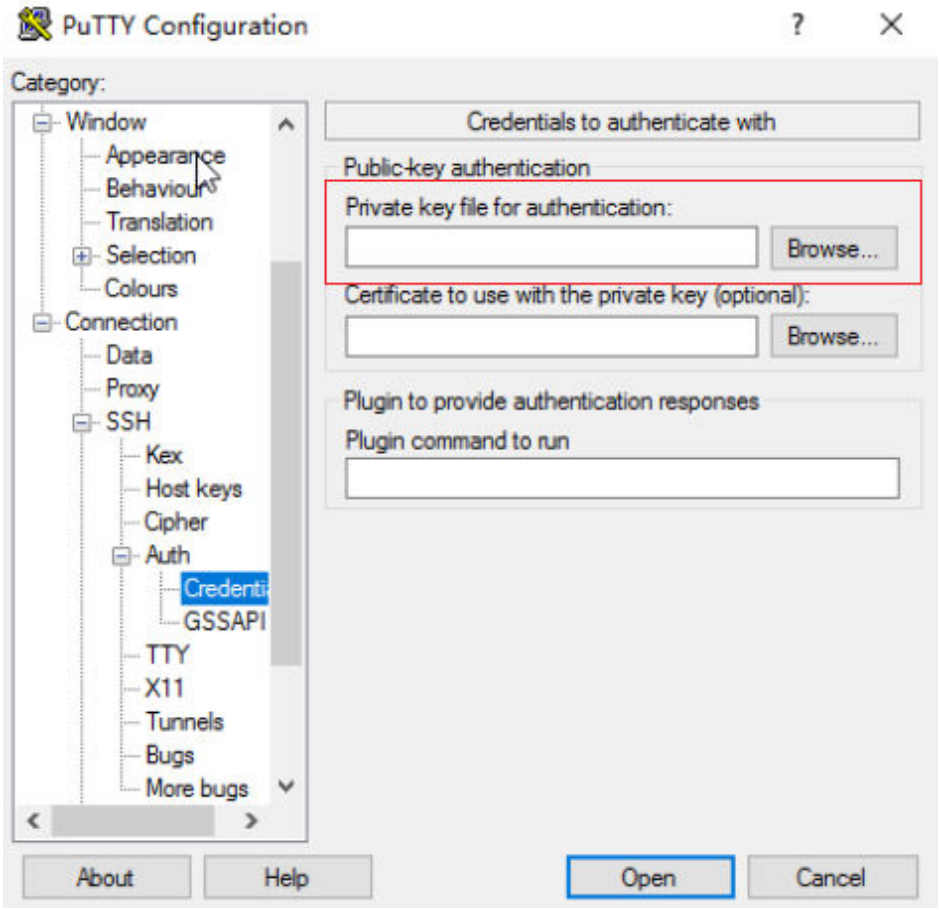
9. Choose **Connection** > **Data**. Enter the Linux cloud server username in **Auto-login username**.

Figure 3-18 Entering the username



10. Choose **Connection** > **SSH** > **Auth** > **Credentials**. In the configuration item **Private key file for authentication**, click **Browse** and select the private key converted in step **6**.

Figure 3-19 Importing the private key file



11. Click **Open**.

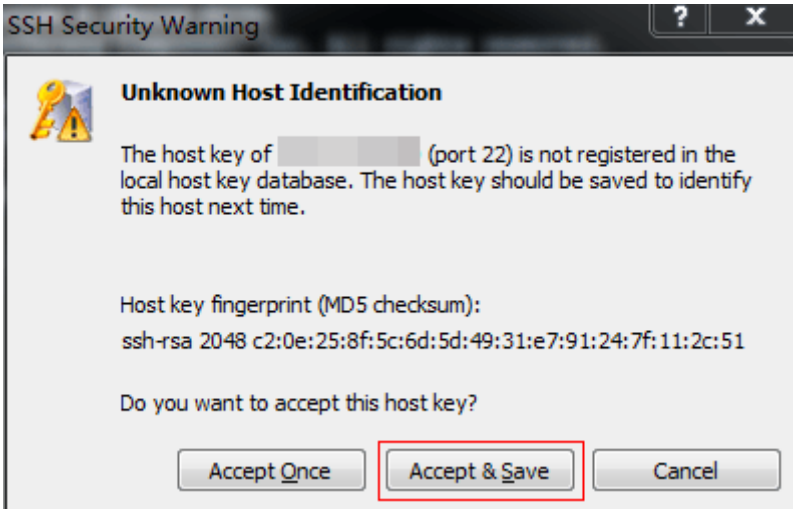
    Log in to the cloud server.

Method 2: Use Xshell to log in to the cloud server.

1. Start the Xshell tool.
2. Run the following command to remotely connect to the cloud server using SSH:

   ssh *Username*@*EIP*
3. (Optional) If the system displays the **SSH Security Warning** dialog box, click **Accept & Save**.

Figure 3-20 SSH security warning



4. Select **Public Key** and click **Browse** beside the user key text box.
5. In the user key dialog box, click **Import**.
6. Select the locally stored key file and click **Open**.
7. Click **OK** to log in to the cloud server.

Logging In to the Linux Instance from a Local Linux Server

Perform the following operations to log in to a Linux server from a local Linux PC. The following procedure uses private key file **kp-123.pem** as an example to log in to the server. The name of your private key file may differ.

1. On the Linux CLI, run the following command to change operation permissions:

   chmod 400 /*path*/kp-123.pem

   In the preceding command, **path** specifies the path where the private key file is saved.

2. Run the following command to log in to the cloud server:

   ssh -i /*path*/kp-123.pem *Default username*@*EIP*

   For example, if the default username is **root** and the EIP is **123.123.123.123**, run the following command:

   ssh -i /*path*/kp-123.pem root@123.123.123.123

   - In the preceding command, **path** specifies the path where the private key file is saved.
   - The EIP is the one bound to the cloud server.

3.5 Logging In to a Linux FlexusL Instance Using an SSH Password

Scenarios

This section describes how to remotely log in to a Linux instance using an SSH password in Windows and Linux.

Prerequisites

- The cloud server is in the running state.
- Port 22 is allowed in the inbound direction of the security group to which the cloud server belongs. For details, see **Configuring Security Group Rules for a FlexusL Instance**.
- The network connection between the login tool (PuTTY) and the target cloud server is normal. For example, the default port 22 is not blocked by the firewall.
- 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**.

Logging In to the Linux Instance from a Local Windows Server

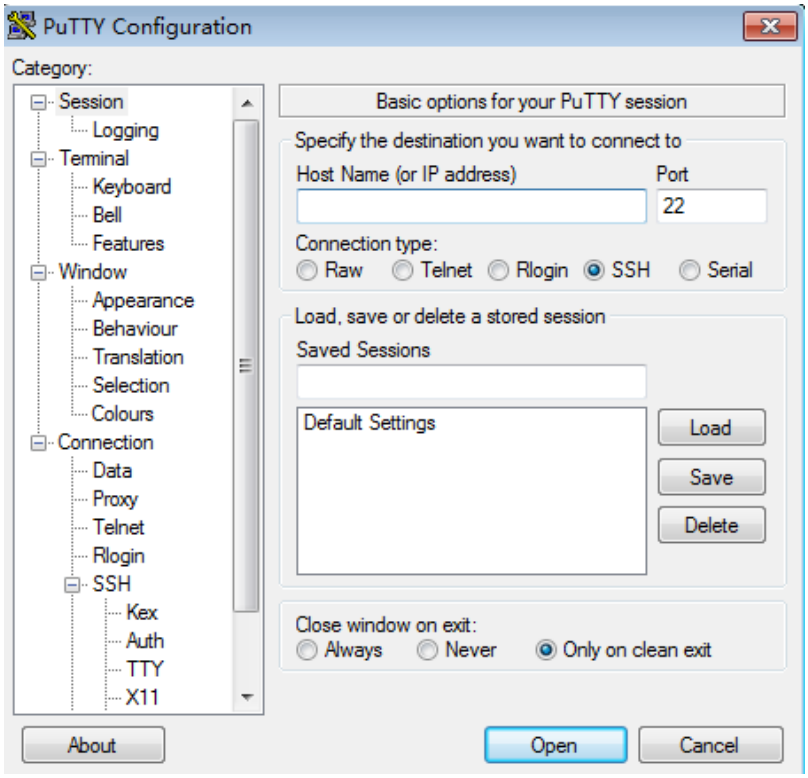
To log in to the Linux instance from a local Windows server, perform the following operations

The following operations use PuTTY as an example to log in to the ECS:

1. Visit the following website and download PuTTY and PuTTYgen:

   https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
2. Run PuTTY.
3. Choose **Session**.
   a. **Host Name (or IP address)**: Enter the EIP bound to the cloud server.
   b. **Port**: Enter **22**.
   c. **Connection type**: Click **SSH**.
   d. **Saved Sessions**: Enter the task name, which can be clicked for remote connection when you use PuTTY next time.

Figure 3-21 Session



4. Choose **Window**. Then, select **UTF-8** for **Received data assumed to be in which character set:** in **Translation**.
5. Click **Open**.

   If you log in to the cloud server for the first time, PuTTY displays a security warning dialog box, asking you whether to accept the cloud server security certificate. Click **Yes** to save the certificate to your local registry.
6. After the SSH connection to the cloud server is set up, enter the username and password as prompted to log in to the cloud server.
   - Username: Enter **root**.
   - **Password**: Enter the password of the cloud server.

     If you forget the password, reset it by referring to **Resetting the Password for a FlexusL Instance**.

Logging In to the Linux Instance from a Local Linux Server

To log in to a Linux instance from a local Linux server, perform the following operations:

1. On the Linux CLI, run the following command to log in to the cloud server:

   ssh *xx.xx.xx.xx*

   NOTE

   xx.xx.xx.xx indicates the EIP bound to the cloud server.
2. Verify the SSH fingerprint of the cloud server and enter **yes**.

   The authenticity of host '*xx.xx.xx.xx* (*xx.xx.xx.xx*)' can't be established.
   ECDSA key fingerprint is SHA256:rnKuzrUSYS03MCoa*xxxxxxxxxxxxxxxxxxxxxxxxxxx*.
   ECDSA key fingerprint is MD5:cf:64:5b:5e:74:30:*xx:xx:xx:xx:xx:xx:xx:xx:xx:xx*.


```
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'xx.xx.xx.xx' (ECDSA) to the list of known hosts.
```

3. Enter the password for logging in to the cloud server.

   If you forget the password, reset it by referring to **Resetting the Password for a FlexusL Instance**.

```
root@xx.xx.xx.xx's password:

      Welcome to Huawei Cloud Service
```


4 Managing FlexusL Instances

4.1 Resetting the Password for a FlexusL Instance

4.1.1 Configuring Custom Policies for FlexusL Self-Service O&M

Scenarios

FlexusL self-service O&M (such as online password reset) depends on Cloud Operations Center (COC). You need to enable and authorize COC first. After COC is enabled and authorized, two agencies "ServiceLinkedAgencyForCOC" and "ServiceAgencyForCOC" will be created and granted permissions required to perform operations on FlexusL instances through COC. For details, see **Enabling COC**.

If you want to perform self-service O&M on FlexusL instances as an IAM user, contact the account which is used to create the IAM user to assign COC permissions to the user.

This section describes how to assign COC permissions to an IAM user.

Prerequisites

The IAM user has been granted FlexusL permissions.

NOTE

If the assigned FlexusL permissions do not meet your requirements, assign permissions to the IAM user by referring to **Granting Permissions to Use FlexusL Instances Through IAM**.

Procedure

1. Log in to the IAM console and access the **Policies/Roles** page using the account.

2. In the upper right corner of the page, click **Create Custom Policy** and assign COC permissions.

   For details, see **Creating a Custom Policy**.

   The following example describes how to add a custom policy for enabling COC and performing operations on COC.

   a. (Optional) Create a custom policy named **Enable COC** and assign the following permissions:

      NOTE

      If the account used to create the IAM user has enabled COC, you can skip this step.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:agencies:list*",
                "iam:agencies:createAgency",
                "iam:agencies:createServiceLinkedAgencyV5",
                "coc:agency:get",
                "coc:agency:create",
                "iam:permissions:grantRoleToAgency",
                "iam:permissions:grantRoleToAgencyOnDomain",
                "iam:roles:listRoles"
            ]
        }
    ]
}
```

   b. Create a custom policy named **COC Operations** and assign the following permissions:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "coc:instance:listResources",
                "coc:application:listResources",
                "coc:schedule:list",
                "coc:schedule:enable",
                "coc:schedule:update",
                "coc:schedule:disable",
                "coc:schedule:approve",
                "coc:schedule:create",
                "coc:schedule:delete",
                "coc:schedule:count",
                "coc:schedule:get",
                "coc:schedule:getHistories",
                "coc:application:GetDiagnosisTaskDetails",
                "coc:application:CreateDiagnosisTask",
                "coc:document:create",
                "coc:document:listRunbookAtomics",
                "coc:document:getRunbookAtomicDetails",
                "coc:document:list",
                "coc:document:delete",
                "coc:document:update",
                "coc:document:get",
                "coc:document:analyzeRisk",
                "coc:instance:autoBatchInstances",
                "coc:instance:executeDocument",
                "coc:instance:start",
                "coc:instance:reboot",
                "coc:instance:stop",
```



```
            "coc:job:action",
            "coc:instance:reinstallOS",
            "coc:instance:changeOS",
            "coc:hostAccount:describe",
            "coc:instance:syncResources"
        ]
    }
  ]
}
```

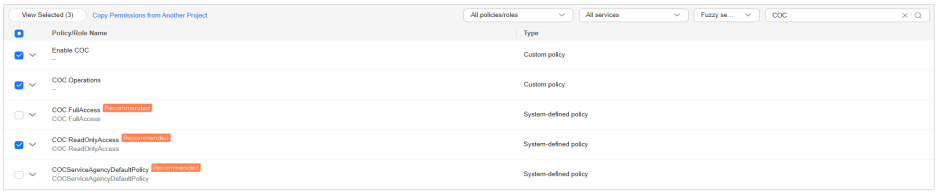
3. Create a user group and assign COC permissions to it.

   For details, see **Creating a User Group and Assigning Permissions**.

   Assign the following permissions to the user group:

   - COC ReadOnlyAccess
   - Custom policy created in **2** for enabling COC and performing operations on COC

   Figure 4-1 Assigning permissions to the user group



4. On the **Users** page of the IAM console, locate the target user and click **Authorize** in the **Operation** to assign COC permissions to the user.

   For details, see **Assigning Permissions to an IAM User**.

   On the displayed page, select the user group created in **3** so that the user inherits permissions from the group.

4.1.2 Resetting the Password of a FlexusL Instance Online or Offline

Scenarios

You can reset a password for one or more FlexusL instances when:

- You use FlexusL instances for the first time. FlexusL instances do not have initial passwords.
- The password is lost or expires.

> **NOTE**
>
> Online password reset is not available in a few regions. Refer to the console display for specific availability.

Constraints

Table 4-1 Constraints on resetting a password

Item	Online Password Reset	Offline Password Reset
Service dependency	Cloud Operations Center (COC) needs to be enabled and authorized. For IAM users, permissions for COC operations need to be granted. For details, see **Configuring Custom Policies for FlexusL Self-Service O&M**.	N/A
Plug-in dependency	The UniAgent plug-in provided by Application Operations Management (AOM) needs to be deployed on FlexusL instances for delivering and executing scripts. If a UniAgent is not installed, being installed, or abnormal, you cannot reset the password online. Install a UniAgent as instructed.	A password reset plug-in is required. • 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. FlexusL instances 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 FlexusL Instance and I Forgot the Initial Password of the Private Image?** • Do not delete password reset processes **CloudResetPwdAgent** and **CloudResetPwdUpdateAgent**, or the password reset will be unavailable.
Supported status	Running	• Running • Stopped

Item	Online Password Reset	Offline Password Reset
Effective time	The new password will be applied immediately after the reset.	Depending on the statuses of FlexusL instances. • Running: The new password is applied after the instance is restarted. **NOTE** • Auto restart may cause data loss. You are advised to stop the FlexusL instance first before resetting the password. • A FlexusL instance restart may cause a service interruption. You are advised to perform the operation during off-peak hours. • Stopped: The new password is applied after the instance is started.
Other	Passwords cannot be reset for FlexusL instances running Windows and Linux in the same batch.	N/A

Prerequisites

Ensure that the FlexusL instance network is normal and DHCP has been enabled for the VPC network used by the instance.

Procedure

You can reset the password online or offline.

- Online password reset: This function depends on COC and the AOM UniAgent plug-in. The password change is applied immediately without restarting FlexusL instances.
- Offline password reset: This function does not depend on COC and the AOM UniAgent plug-in. The password change is applied only after FlexusL instances are restarted or started.

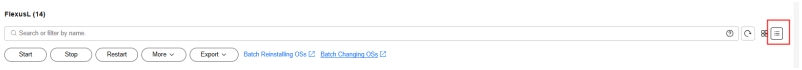
Online Password Reset

1. Log in to the FlexusL **console**.
2. Reset the password for one or more FlexusL instances.

NOTE

By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

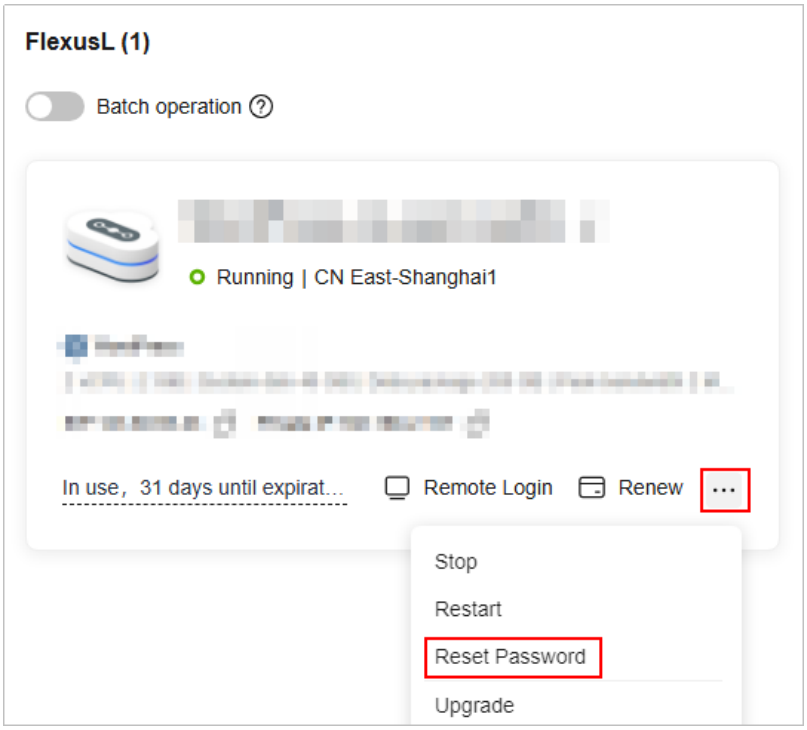
Figure 4-2 Switching views



– Resetting the password for logging in to a single FlexusL instance using any of the following methods:

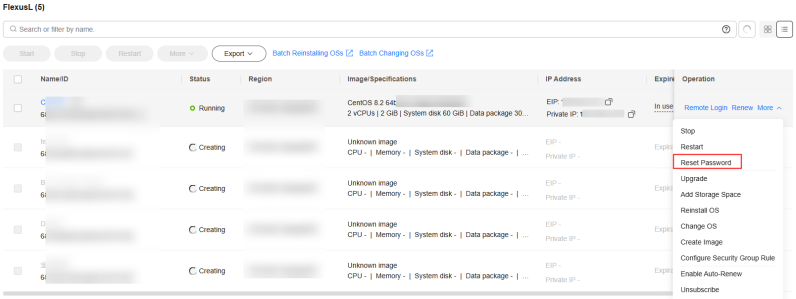
  - In the card view, choose ··· > **Reset Password** on the resource card.

    Figure 4-3 Resetting the password from the resource card

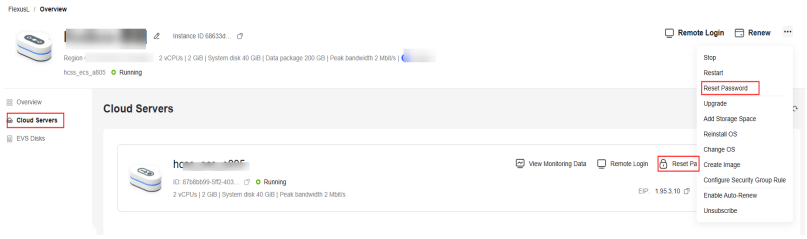
  - In the list view, locate the target FlexusL instance and choose **More** > **Reset Password** in the **Operation** column.

    Figure 4-4 Resetting the password from the list page

- Click the target resource card or instance name to go to the instance details page. In the navigation pane on the left, choose **Cloud Servers**, locate the target server, and click **Reset Password**.

  Figure 4-5 Resetting the password for an individual instance

– Batch resetting passwords

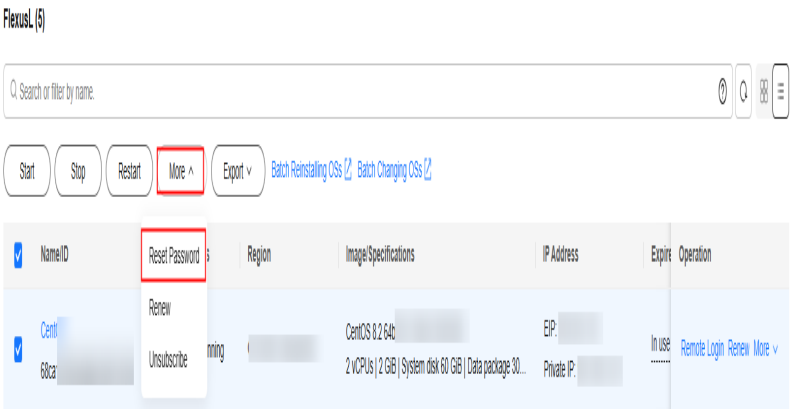
  In the card view, enable **Batch operations**, click **Select all** or select the target instances, and choose **More** > **Reset Password**.

  Figure 4-6 Resetting passwords for multiple instances

  In the list view, select the target instances and choose **More** > **Reset Password** above the instance list.

  Figure 4-7 Resetting passwords from the list page

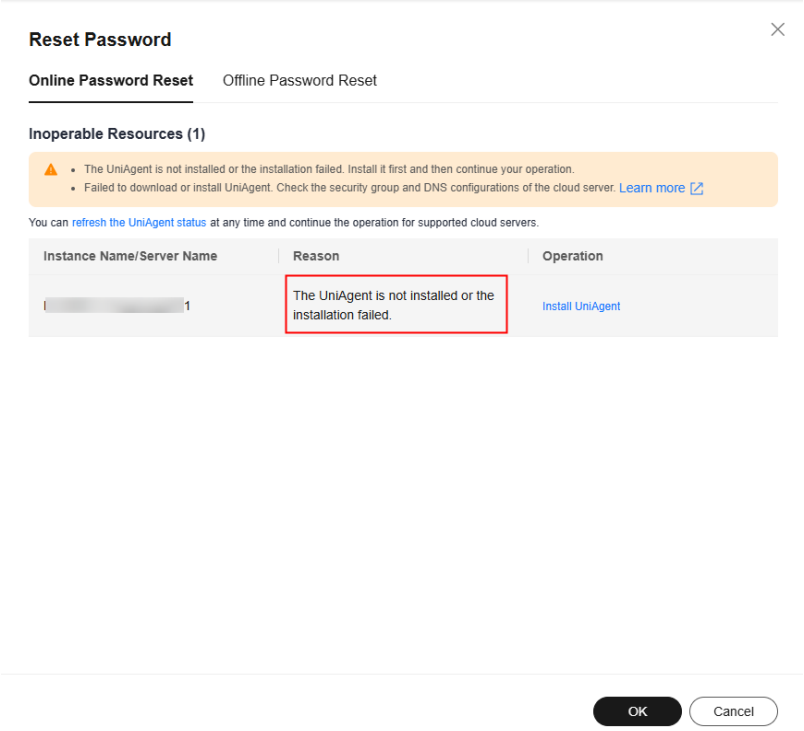
  After the passwords are reset in a batch, the passwords for logging in to these instances are the same.

3. Click the **Online Password Reset** tab.
4. (Optional) On the **Enable COC and Grant Permissions** page, read and agree to the service statement, and click **Enable and Authorize**.

   This page is displayed if COC is not enabled and authorized.

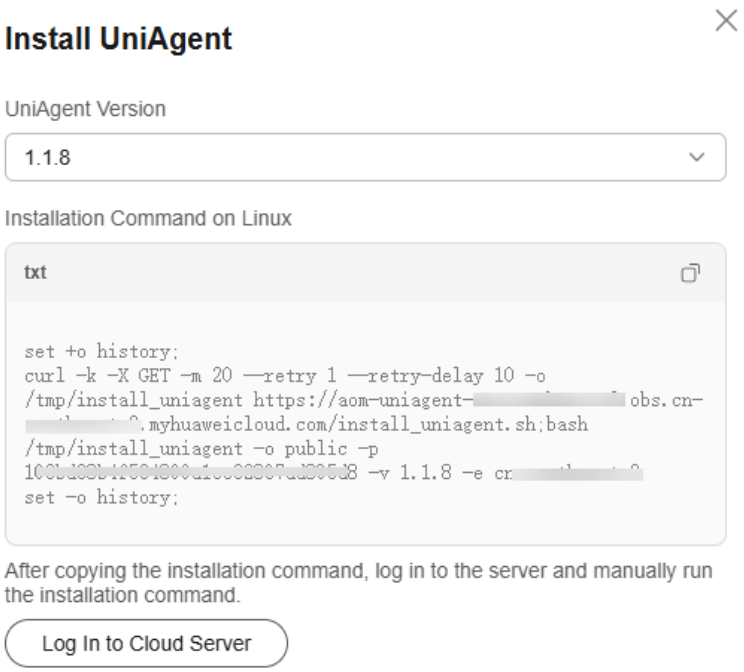
5. (Optional) If UniAgents are not installed or an exception occurs during the installation, log in to the FlexusL instances and install UniAgents on FlexusL instances as instructed.

Figure 4-8 Message displayed



a. Click **Install UniAgent** in the **Operation** column.

Figure 4-9 Installing UniAgent (Linux OS used as an example)



b. Select a UniAgent version. The latest version is recommended.

c. Click the copy button in the upper right corner of the installation command area to copy the installation command.

d. Click **Log In to Cloud Server**.

e. Run the UniAgent installation command on the FlexusL instances.

   - For FlexusL instances running Windows, download the installation package and install UniAgents as instructed.
   - For FlexusL instances running Linux: paste and execute the installation command copied in step **5.c**.

f. Return to the **Online Password Reset** tab and click **refresh the UniAgent status** to check the UniAgent installation status.

   UniAgent installation and status synchronization take several minutes. After UniAgents are installed, you can perform the subsequent operations.

6. Configure the required parameter settings.

Figure 4-10 Resetting the password online

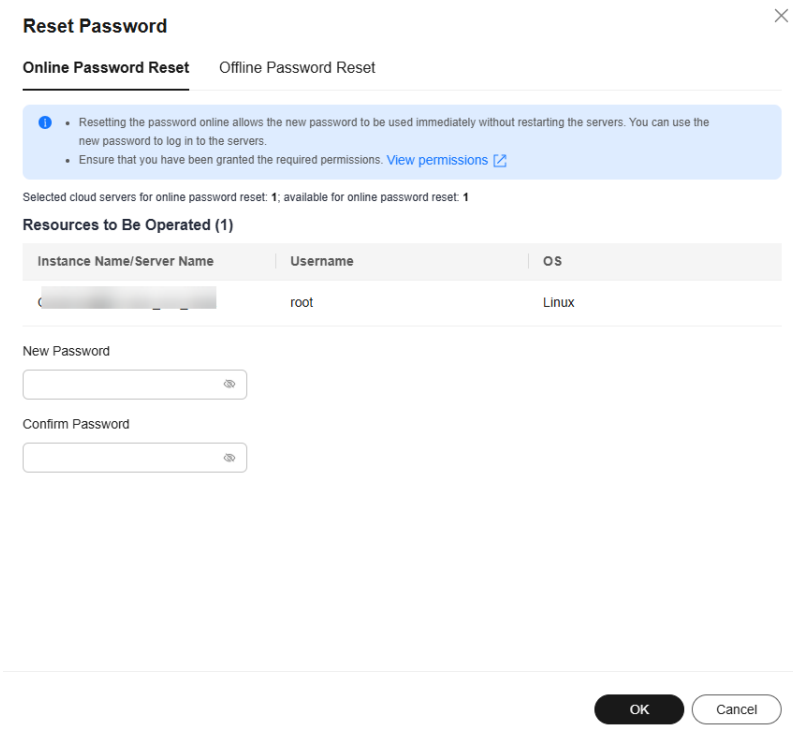


Table 4-2 Parameters for resetting the password online

Parameter	Description
New Password	The new password. The new password must comply with the following rules: • Must contain 8 to 26 characters. • Must contain at least three of the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters Linux: @%-_=+[]:./^,{}? Windows: $@%-_=+[]:./,? • Cannot contain the username or the username spelled backwards. • Cannot contain more than two consecutive characters in the username (only applied to Windows). • Cannot start with a slash (/) (only applied to Windows).

Parameter	Description
Confirm Password	Must be the same as the new password.

7. Click **OK**.

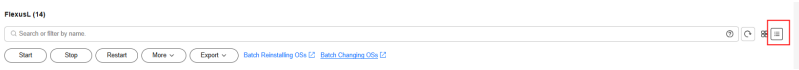
Offline Password Reset

1. Log in to the FlexusL **console**.
2. Reset the password for one or more FlexusL instances.

   NOTE

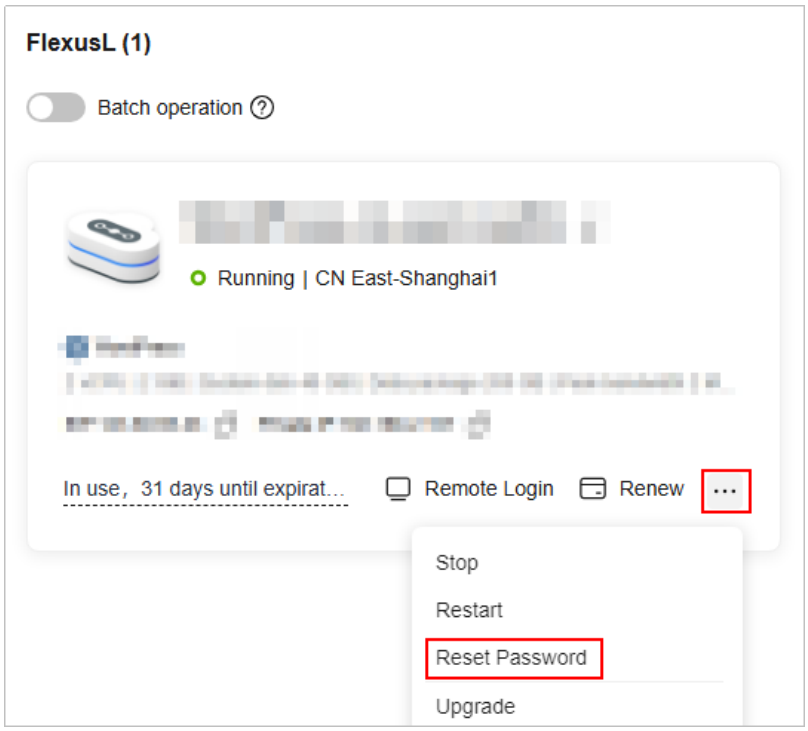
   By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

   Figure 4-11 Switching views

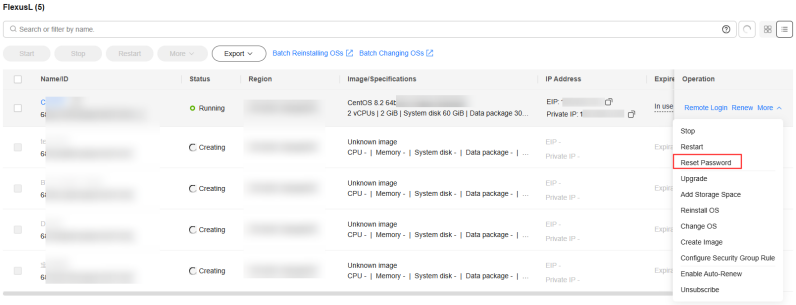
   - Resetting the password for logging in to a single FlexusL instance using any of the following methods:
     - In the card view, choose ··· > **Reset Password** on the resource card.

       Figure 4-12 Resetting the password from the resource card

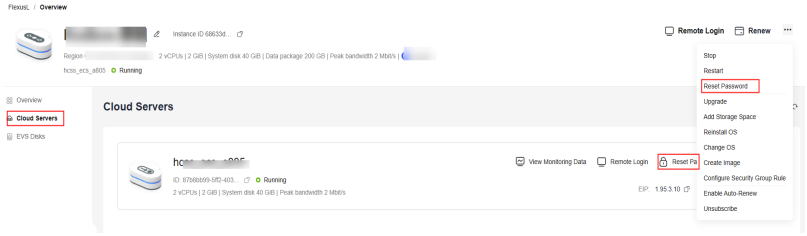
     - In the list view, locate the target FlexusL instance and choose **More** > **Reset Password** in the **Operation** column.

Figure 4-13 Resetting the password from the list page



- Click the target resource card or instance name to go to the instance details page. In the navigation pane on the left, choose **Cloud Servers**, locate the target server, and click **Reset Password**.

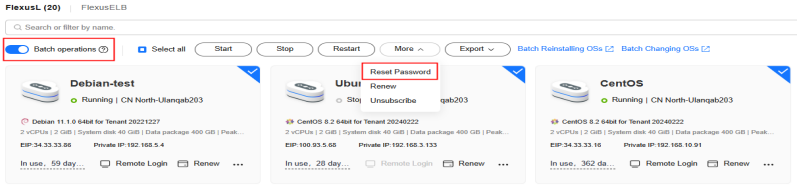
Figure 4-14 Resetting the password for an individual instance



– Batch resetting passwords

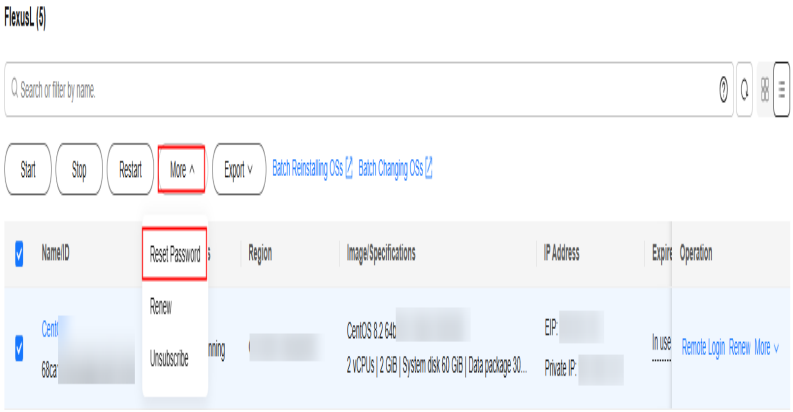
  In the card view, enable **Batch operations**, click **Select all** or select the target instances, and choose **More** > **Reset Password**.

Figure 4-15 Resetting passwords for multiple instances



In the list view, select the target instances and choose **More** > **Reset Password** above the instance list.

Figure 4-16 Resetting passwords from the list page



After the passwords are reset in a batch, the passwords for logging in to these instances are the same.

3. Set and confirm a new password as instructed.

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

Figure 4-17 Resetting the password offline

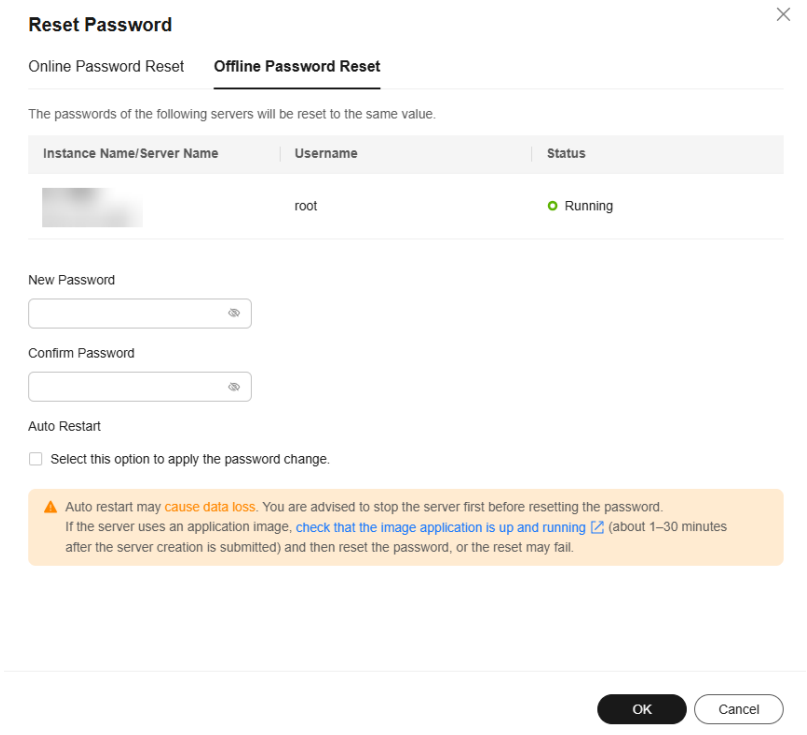


Table 4-3 Parameters for password reset

Parameter	Description
New Password	The new password. The new password must comply with the following rules: • Must contain 8 to 26 characters. • Must contain at least three of the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters Linux: !@%-_=+[]:./? Windows: !@%-_=+[]:./? • Cannot contain the username or the username spelled backwards. • Cannot contain more than two consecutive characters in the username (only applied to Windows). • Cannot start with a slash (/) (only applied to Windows).
Confirm Password	Must be the same as the new password.

4. Click **OK**.

   The password change will be applied after the instance is restarted. Log in to the instance to verify the new password.

   NOTE

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

Helpful Links

- **Remotely Logging In to a FlexusL Instance**
- **Where Can I Find the Username and Password for Remotely Logging In to a FlexusL Instance?**
- **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 FlexusL 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 FlexusL Instance and I Know the Initial Password of the Private Image?**

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 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 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.

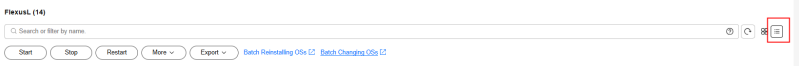
Procedure

1. Log in to the FlexusL **console**.
2. Reinstall the OS using any of the following methods:

   NOTE

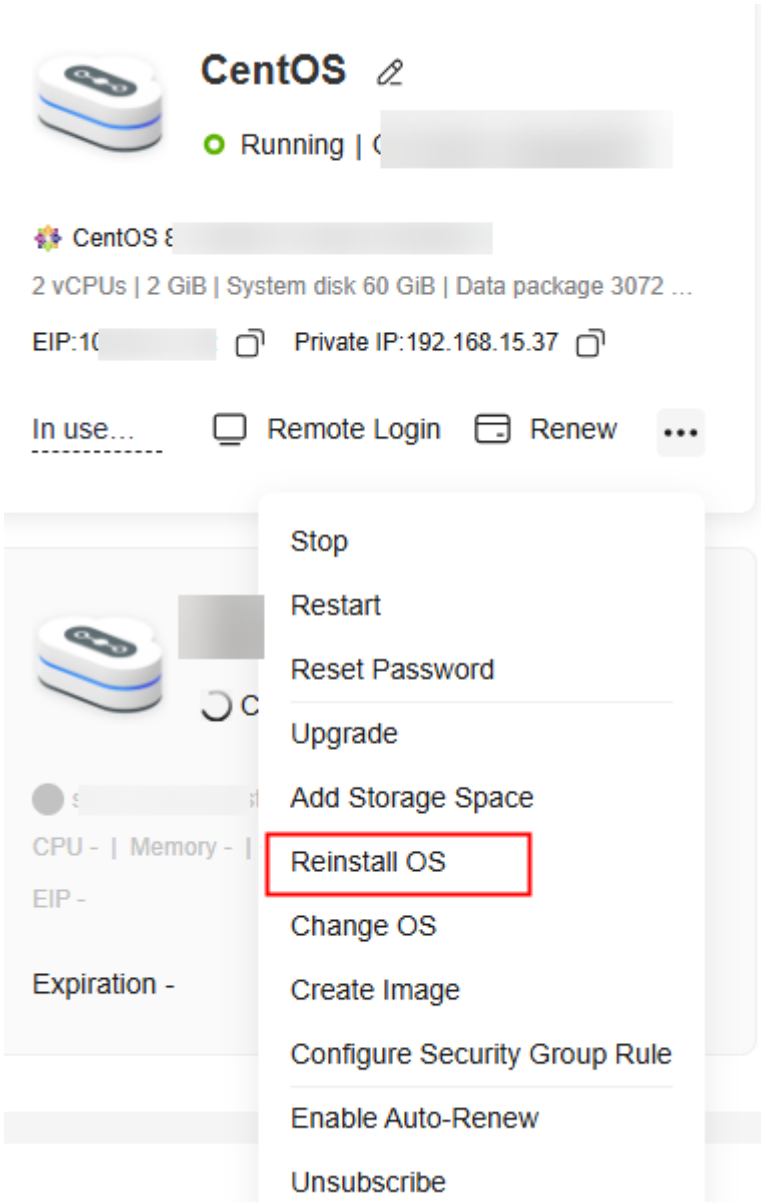
   By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

   Figure 4-18 Switching views

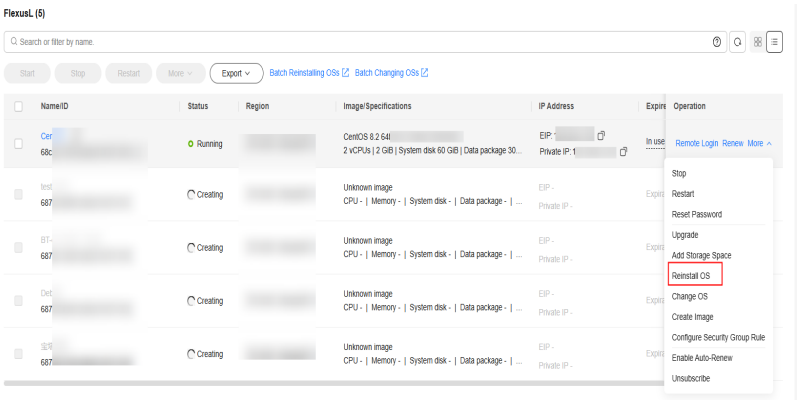
   - Method 1: In the card view, choose ··· > **Reinstall OS** on the resource card.

Figure 4-19 Reinstalling an OS from the resource card



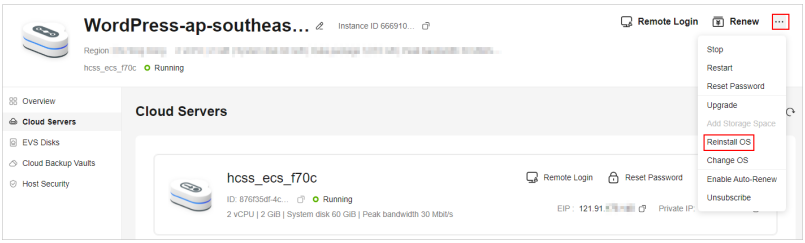
- Method 2: In the list view, locate the target FlexusL instance and choose **More** > **Reinstall OS** in the **Operation** column.

Figure 4-20 Reinstalling an OS from the list page

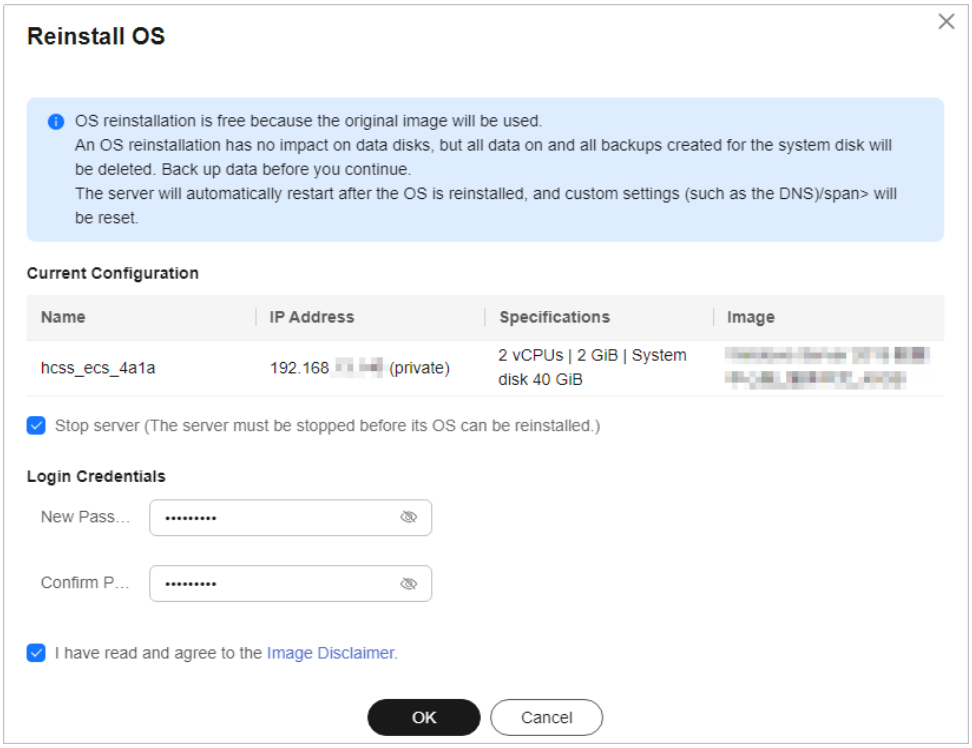


– Method 3: On the **Cloud Servers** details page, choose > **Reinstall OS**.

Figure 4-21 Reinstalling an OS on the details page



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

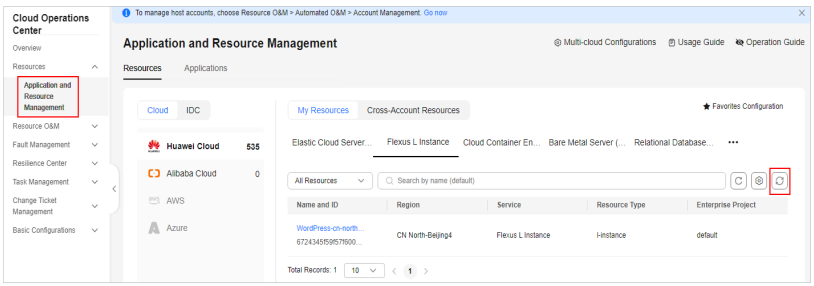
Before reinstalling OSs, make the following preparations:

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. Obtain 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 4-22 Synchronizing FlexusL instance resources



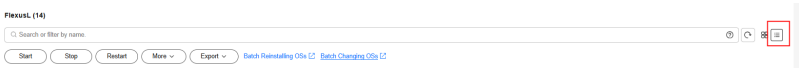
Procedure

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

   NOTE

   By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

   Figure 4-23 Switching views

2. In the card view, enable **Batch operation** and click **Batch Reinstalling OSs**.

   In the list view, click **Batch Reinstalling OSs** above the instance list.

   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 4-24 Batch reinstalling OSs in the card view

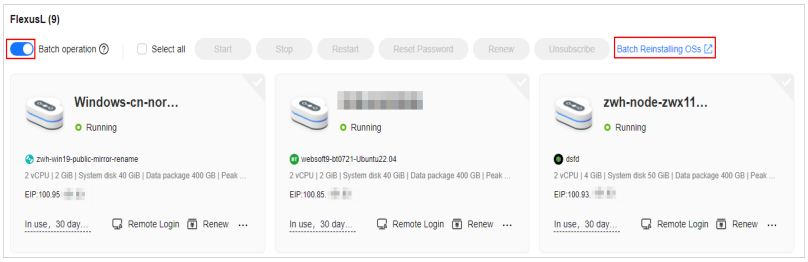
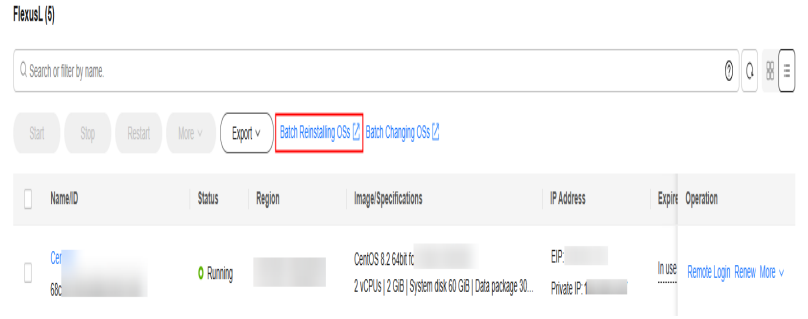
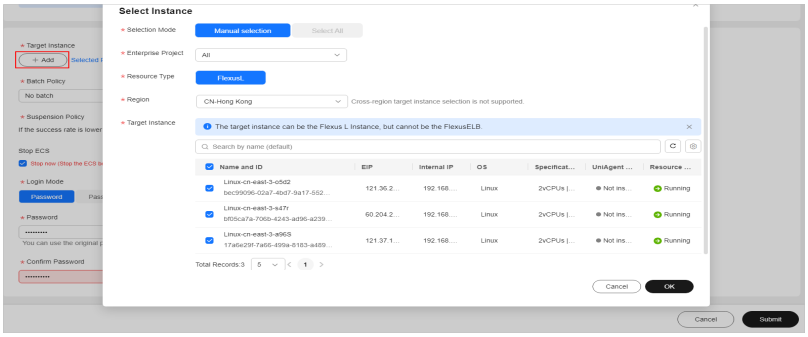


Figure 4-25 Batch reinstalling OSs in the list view



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

Figure 4-26 Batch reinstalling OSs



Parameter	Description
Target Instance	• **Selection Mode**: **Manual selection** (only this option supported) • **Enterprise Project**: **All** • **Resource Type**: fixed to **FlexusL**, indicating that OSs are batch reinstalled for FlexusL instances • **Region**: Select the region where FlexusL instances are located. The instances must be in the same region. Batch OS reinstallation is not available for FlexusL instances in different regions. • **Target Instance**: Select the FlexusL instances whose OSs are to be reinstalled. If some FlexusL instances are missing in the list, **synchronize resources first**.
Batch Policy	Select a batch policy based on your requirements. • **Automatic**: The selected FlexusL instances are automatically divided into multiple batches based on the preset rule. • **Manual**: You can manually create multiple batches and add FlexusL instances to each batch as required. • **No batch**: All selected FlexusL instances will be executed in the same batch. **NOTE** • If you select **Automatic** or **Manual** and multiple batches of OS reinstallation tasks are generated, the process will be suspended after each batch of tasks is executed. You need to manually continue the next batch. For details, see **Related Operations**. • If there are services running on your FlexusL instances, the **No batch** policy may affect your services. You are advised to select the automatic or manual batch policy.
Suspension Policy	Determine the policy for suspending a task. You can set the success rate of OS reinstallation. When the success rate is lower than the specified value, the task status becomes abnormal and the task is suspended. The value is from 0 to 100 and can be accurate to one decimal place. Success rate = (Number of FlexusL instances whose OSs are successfully reinstalled/Total number of FlexusL instances) x 100%
Stop ECS	This option is displayed when there are FlexusL instances in **Running** state. Select **Stop now**.
Login Mode	• **Password**: Set a unified password for logging in to FlexusL instances whose OSs are to be installed. • **Reset password**: Reset the password by performing **Resetting the Password for a FlexusL Instance** when logging in to the FlexusL instances for the first time.

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

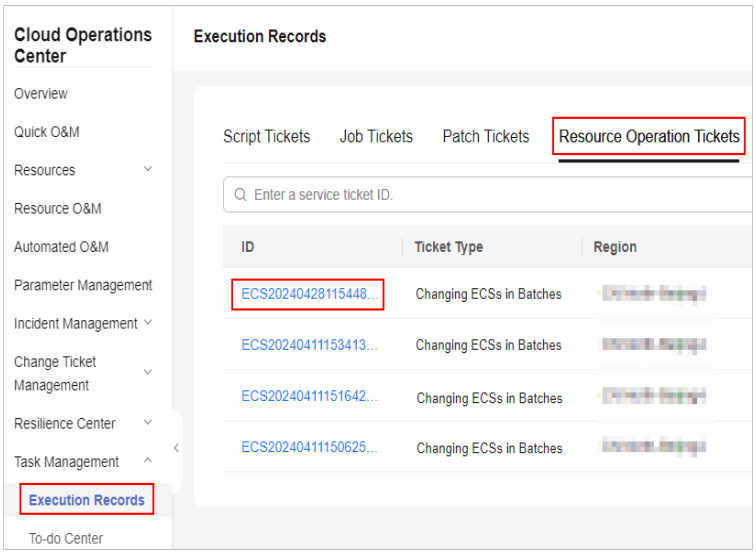
   After the OS is reinstalled, the cloud server will automatically restart. When the server status is **Running**, the OS reinstallation is complete.

   After the request is submitted, the system generates a service ticket and you will be automatically redirected to the page in **Figure 4-27**. You can also **view the service ticket details** later.

Related Operations

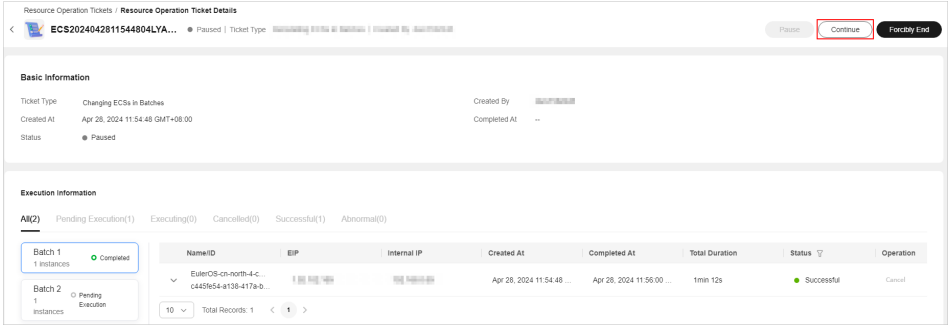
If you select **Automatic** or **Manual** and multiple batches of OS reinstallation tasks are generated, the process will be suspended after each batch of tasks is executed. Perform the following operations to manually continue the next batch of tasks:

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 4-27 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

- If the system disk is not in use, the image cannot be changed.
- The image cannot be changed in the following scenarios:
  - Application images have the minimum CPU and memory specification requirements. If a FlexusL instance has small specifications of vCPUs and memory, you cannot change its OS using an application image that requires higher specifications. For example, you cannot use the GitLab application image that needs at least 2 vCPUs and 8 GiB of memory to change the OS of a FlexusL instance with 2 vCPUs and 4 GiB of memory. To do so, you need to upgrade the FlexusL instance by performing operations described in **Modifying the Specifications of a FlexusL Instance** first.
  - You cannot use the current image of the current version to change the OS of an instance. In this case, you can reinstall the OS. For details, see **Reinstalling the OS of a FlexusL Instance** or **Batch Reinstalling OSs of FlexusL Instances**.
- 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 5-1** 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.

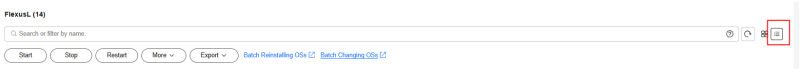
Procedure

1. Log in to the FlexusL **console**.
2. Reinstall the OS using any of the following methods:

   NOTE

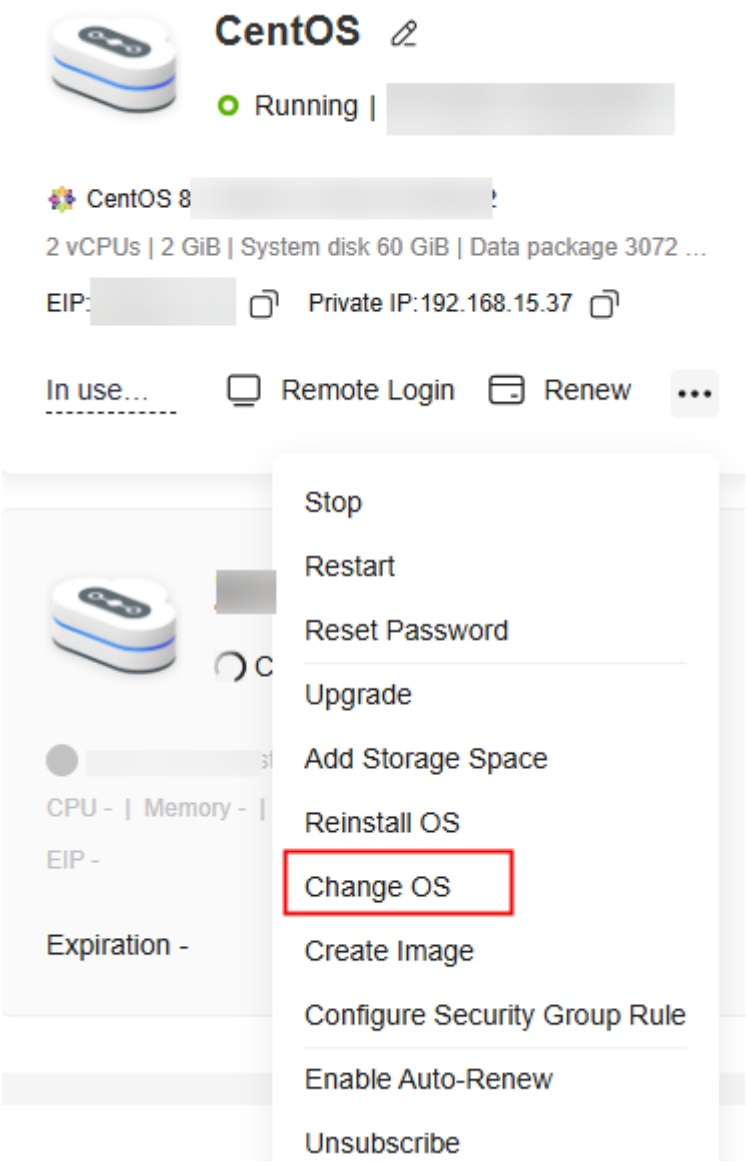
   By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

   Figure 4-28 Switching views

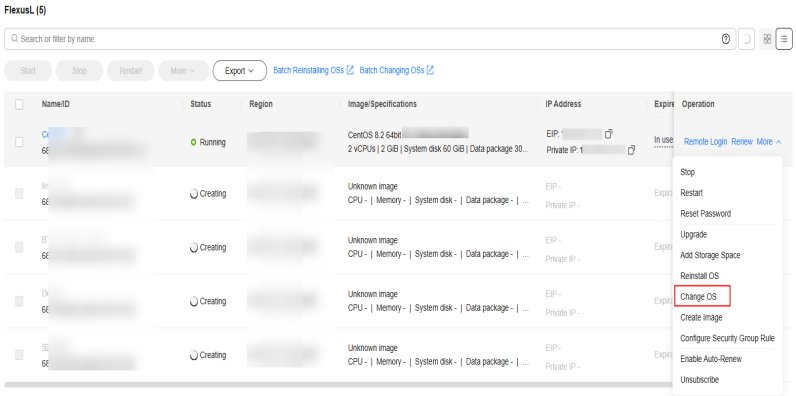
   – Method 1: In the card view, choose ··· > **Change OS** on the resource card.

Figure 4-29 Changing an OS from the resource card

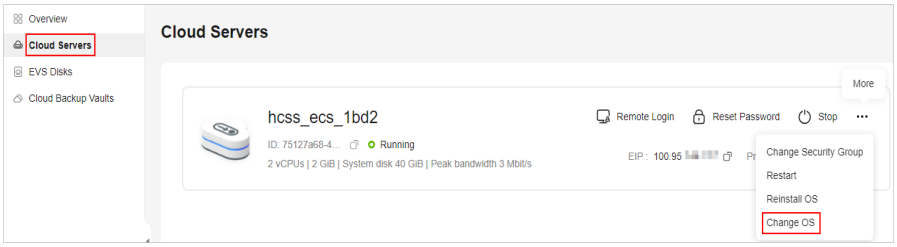


- Method 2: In the list view, locate the target FlexusL instance and choose **More** > **Change OS** in the **Operation** column.

Figure 4-30 Changing an OS from the list page



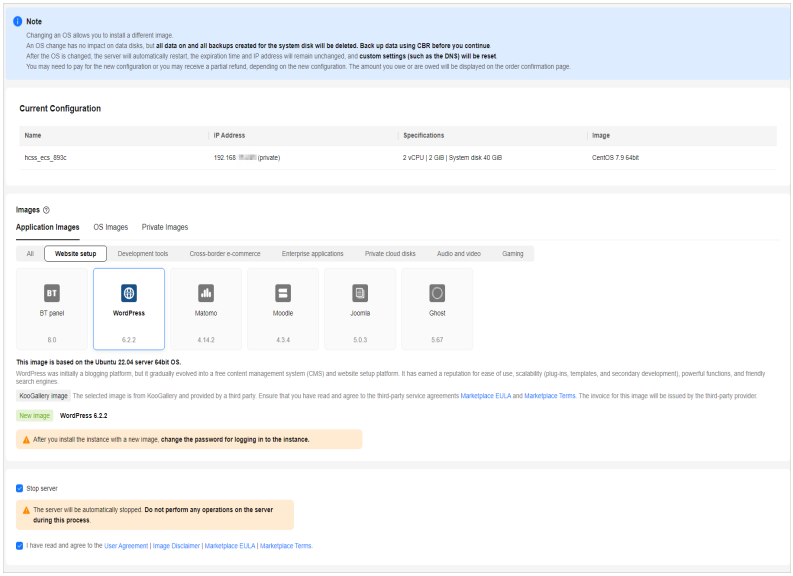
– Method 3: On the **Cloud Servers** details page, choose ··· > **Change OS**.



3. Specify the parameters required for changing the OS.
   – Select the image to be switched.

     FlexusL provides **OS images**, **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.

NOTE

- 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 FlexusL 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 FlexusL 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 with Host Security (HSS) included, HSS will not protect the instance. You need to 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.
- If the system disk is not in use, the image cannot be changed.
- The image cannot be changed in the following scenarios:
  - Application images have the minimum CPU and memory specification requirements. If a FlexusL instance has small specifications of vCPUs and memory, you cannot change its OS using an application image that requires higher specifications. For example, you cannot use the GitLab application image that needs at least 2 vCPUs and 8 GiB of memory to change the OS of a FlexusL instance with 2 vCPUs and 4 GiB of memory. To do so, you need to upgrade the FlexusL instance by performing operations described in **Modifying the Specifications of a FlexusL Instance** first.
  - You cannot use the current image of the current version to change the OS of an instance. In this case, you can reinstall the OS. For details, see **Reinstalling the OS of a FlexusL Instance** or **Batch Reinstalling OSs of FlexusL Instances**.
- 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 5-1** for FlexusL instances.

Preparations

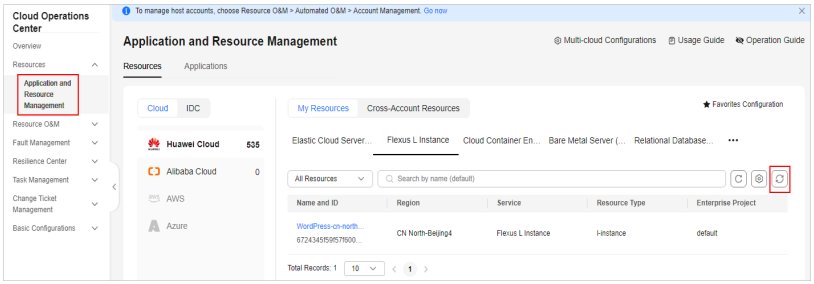
Before batch OS changes, make the following preparations:

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. Obtain 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 4-31 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**.

   NOTE

   By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

   Figure 4-32 Switching views

2. In the card view, enable **Batch operation** and click **Batch Changing OSs**.

   In the list view, click **Batch Changing OSs** above the instance list.

   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 4-33 Batch changing OSs in the card view

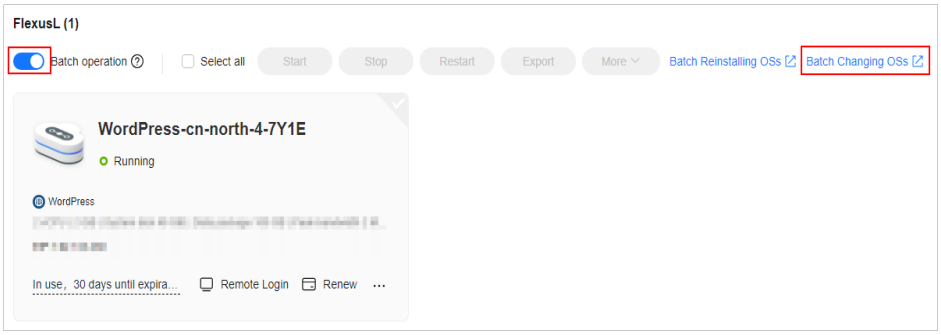
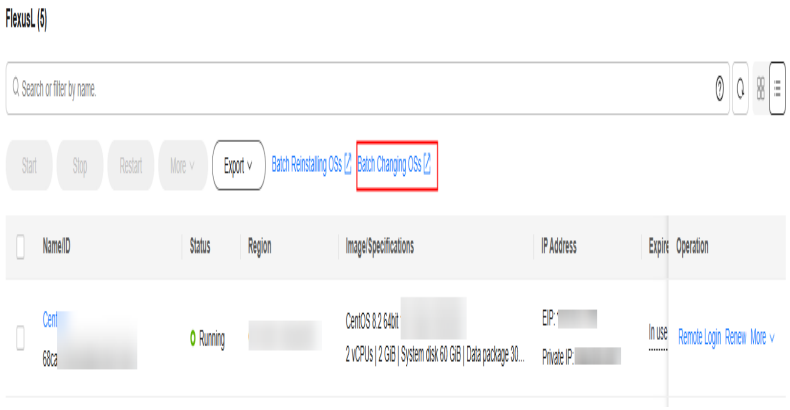
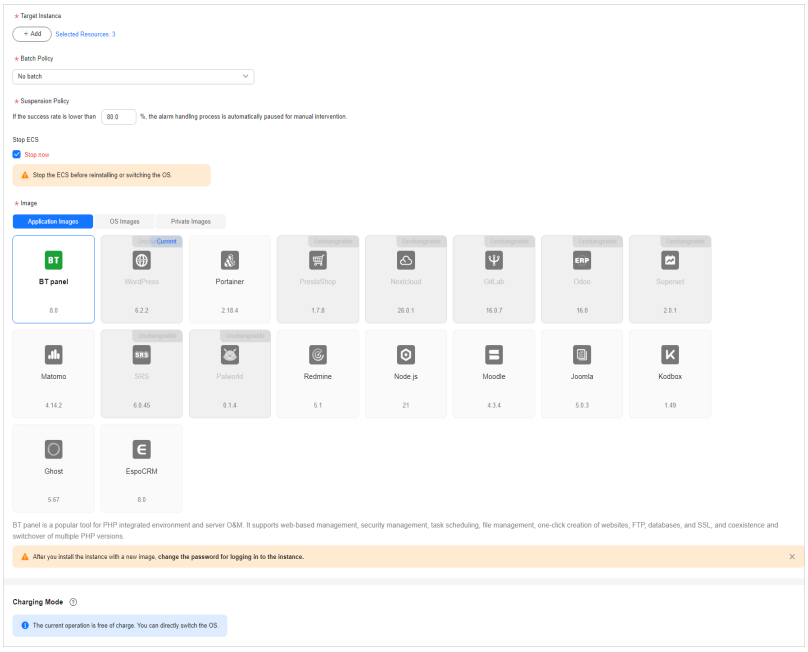
   

Figure 4-34 Batch changing OSs in the list view



3. On the displayed page, configure parameters required for batch OS changes.

Figure 4-35 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**.
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**.

Parameter	Description
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**.

4. 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.

   NOTE

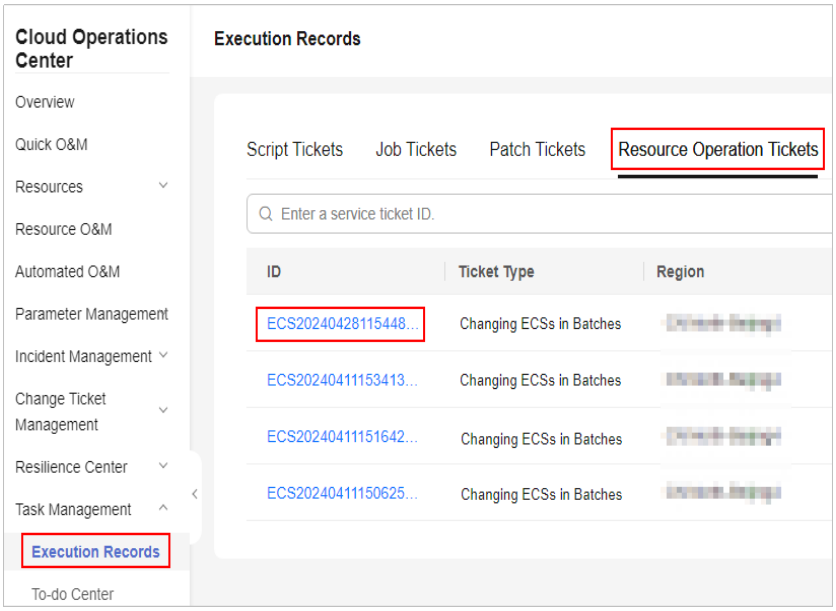
   - Do not reset the password of, restart, or stop the FlexusL instance immediately after the OS is changed. Wait for several minutes until the system successfully injects the password, or the login will fail.
   - After the OS is changed, the login password is cleared. You need to reset the password by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

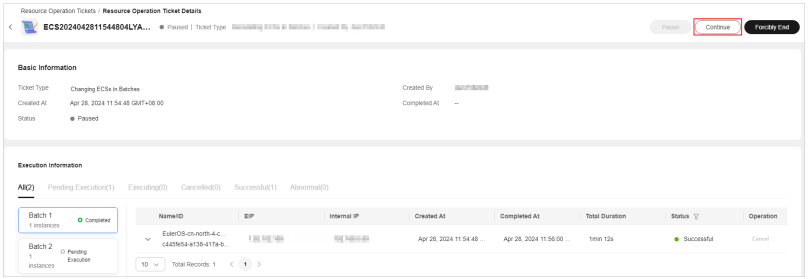
1. Log in to the **COC** console.
2. Choose **Task Management** > **Execution Records**. On the **Resource Operation Tickets** tab, click the target service ticket ID.

Figure 4-36 Viewing execution records



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

Figure 4-37 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 4-4 Unsupported upgrade

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

Constraints

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

Change Impact

Table 4-5 Change impact

Item	Impact
System disks	If the system disk capacity expansion is required, no additional operations like extending partitions or file systems are needed. Your existing data remains unchanged. If the new system disk capacity is already displayed on the console but the file systems are not expanded after you log in to the instance, you can expand the file system manually by referring to the following instructions: • For Windows, see **Extending Disk Partitions and File Systems (Windows)**. • For Linux, see **Extending Disk Partitions and File Systems (Linux)**.
Data Package	The used traffic remains unchanged. The monthly data package quota is changed to that of the new specifications.
Services	You need to stop the server before modifying the specifications. You are advised to modify the specifications during off-peak hours.
Other	After the specifications are modified, the server expiration time and IP address remain unchanged, and the data on the system and data disks is not affected. Other resources are upgraded based on the new specifications.

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**.

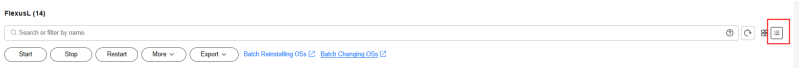
Procedure

1. Log in to the FlexusL **console**.
2. Upgrade the FlexusL instances using any of the following methods:

   NOTE

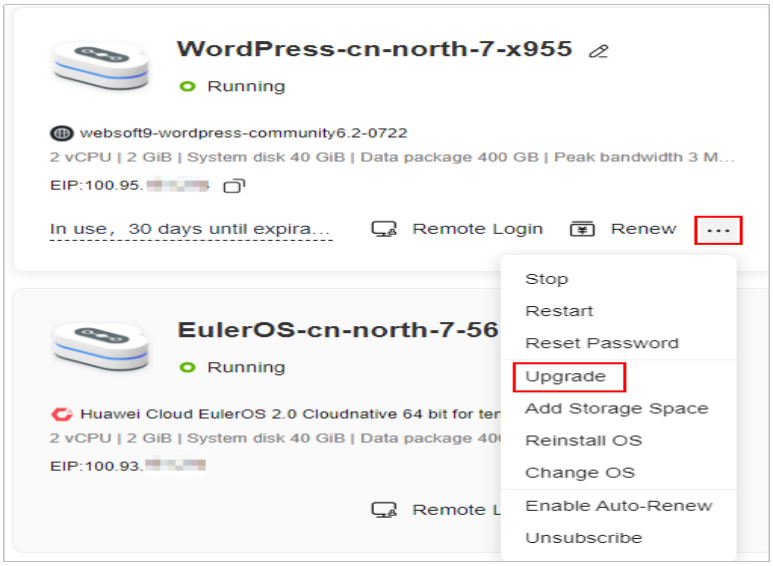
   By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

   Figure 4-38 Switching views

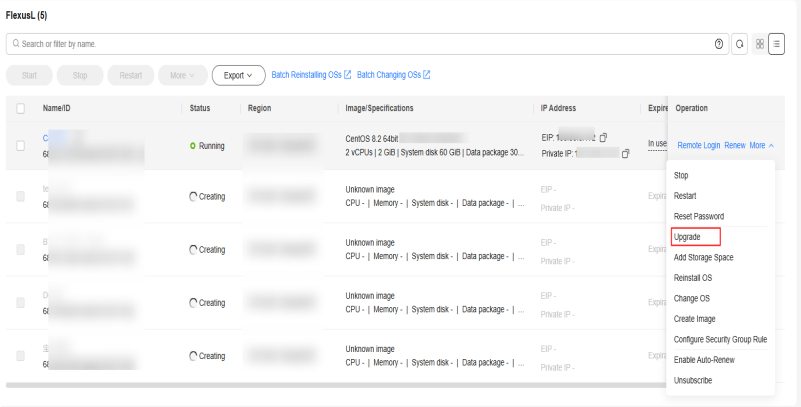
   - In the card view, locate the target resource card and choose ··· > **Upgrade**.

     Figure 4-39 Upgrading an instance from the resource card

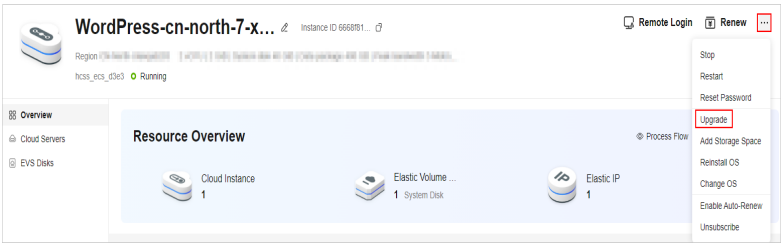
   - In the list view, locate the target FlexusL instance and choose **More** > **Upgrade** in the **Operation** column.

Figure 4-40 Upgrading an instance from the list page



– On the instance details page, choose ··· > **Upgrade** in the upper right corner.

Figure 4-41 Upgrading an instance from the details page



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.

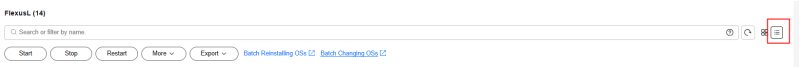
Procedure

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

NOTE

By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

Figure 4-42 Switching views



2. View the FlexusL instance details.

Table 4-6 FlexusL instance details

Item	Description
Data Package	• Expiration time: A FlexusL instance provides a monthly data package. The traffic quota included in the data package is reset each month. Any unused portion of the data package cannot be rolled over to the next month. For example, if you purchase a FlexusL instance for three months at 10:00:00 on June 5, the monthly data package will be valid from 10:00:00 on June 5 to 00:00:00 on July 6. In the next month, the data package will be valid from 00:00:00 on July 6 to 00:00:00 on August 6. In the last-month, the data package will be valid from 00:00:00 on August 6 to 00:00:00 on September 6. • Available: The remaining traffic in the monthly data package. • Used: The traffic volume that has been used in the current month. • Traffic usage: The traffic usage in the current month, which can be calculated using the following formula: Traffic usage = Used traffic/Total traffic volume in a data package
Network	An EIP and a private IP address.
Server	The name, status, and operation entries of the cloud server.
Image	OS installed on the cloud server.
Data Monitoring	Common monitoring information. For more information, see **Monitoring FlexusL Instances Using Cloud Eye**.

3. In the navigation pane on the left, choose **Cloud Servers** to view server overview information.

Table 4-7 Cloud server overview

Server Details	Description
Name/ID	Cloud server name or ID

Server Details	Description
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 • **View Monitoring Data**: Go to the Cloud Eye console to view the monitoring metrics of the FlexusL instance. For more information, see **Monitoring FlexusL Instances Using Cloud Eye**. • **Remote Login**: Select a login mode as required. For more information, see **Login Modes**. • **Reset Password**: A FlexusL instance does not have an initial password. You will have to **reset a password**. • **Stop**: Stop the FlexusL instance. • **Configure Security Group Rule**: For details, see **Configuring the Security Group for a FlexusL Instance**. • Restart: Restart the FlexusL instance. • **Reinstall OS**: If the OS of the cloud server is abnormal, reinstall the OS. For details, see **Reinstalling the OS of a FlexusL Instance**. • **Change OS:** Change the OS of the FlexusL instance. For details, see **Changing an OS**.

4. 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.

Table 4-8 Cloud server details

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 **Adding and Resolving a Domain Name for a FlexusL Instance**.
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, VPC ID, and creation time. The value of a property is the property value.

Figure 4-43 Properties and values

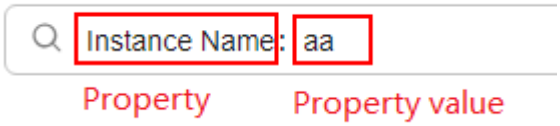
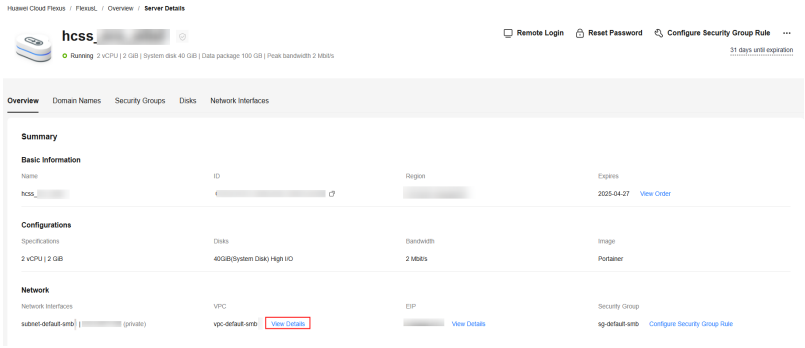
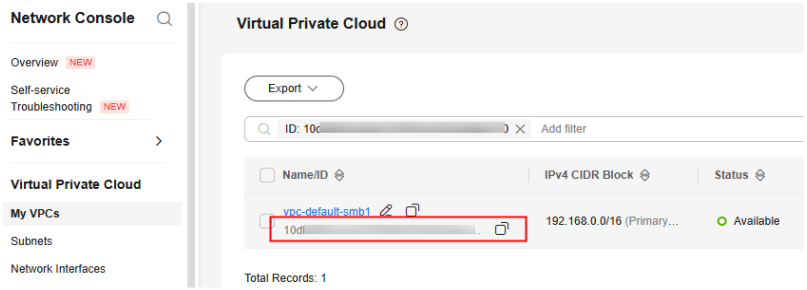


Table 4-9 describes each property.

Table 4-9 Property description

Property	Description
Instance name	Name of a FlexusL instance.
Instance ID	ID of a FlexusL instance.
EIP	Public IP address of a FlexusL instance.
Server ID	ID of the cloud server in a FlexusL instance. Figure 4-44 shows the instance ID and cloud server ID on the FlexusL console. **Figure 4-44** Instance ID and cloud server ID 

Property	Description
VPC ID	ID of the VPC that a FlexusL instance belongs to. On the **Overview** page of the FlexusL instance, click **View Details** next to the VPC to go to the VPC console. **Figure 4-45** Querying details about a VPC  **Figure 4-46** Obtaining the VPC 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, VPC ID, and creation time) only support exact search, which means you must enter a complete property value.
- You cannot search for multiple instance names at the same time.

Procedure

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

NOTE

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

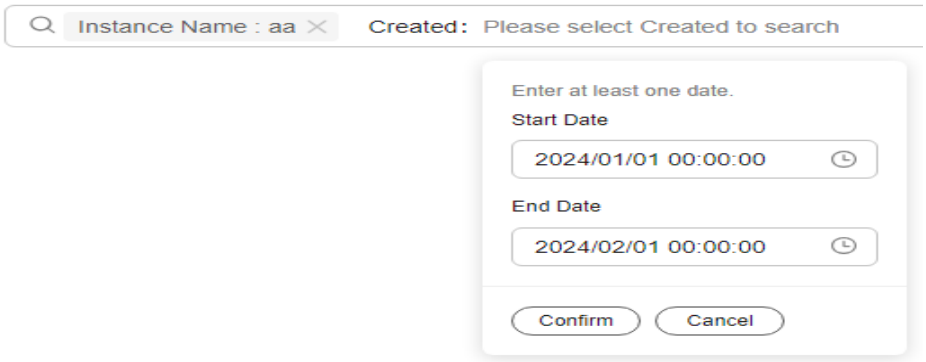
You can also manually select one or more properties and enter or select property values.

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

- Example 2: Searching by a single property with multiple values
  You can select the same property for multiple times and enter or select property values. Alternatively, you can select a property, enter multiple property values and separate them with commas (,). Multiple property values of a single property are in OR relationship.
  a. Select a property from the search box, enter multiple property values, and separate them with commas (,).
     For example, select the EIP property and enter **1.1.1.1,1.1.1.2** to search for the FlexusL instances whose EIP is 1.1.1.1 or 1.1.1.2.

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

- Example 3: Searching by multiple properties with multiple values
  You can search by multiple properties and the properties are in AND relationship.
  a. In the search box, select a property and select or enter a property value, and press **Enter**.
     For example, select the instance name property and enter **aa**.
  b. Add another property and value, and press **Enter**.
     For example, select the creation time property and select a start date and end date. Then the FlexusL instances whose names contain **aa** and created within the specified time range are displayed.



4.4.3 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. In the card view, enable **Batch operation** and click **Export** to export all or selected data as required.

   In the list view, click **Export** above the list to export all or selected data as required.

   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.

Figure 4-47 Export in the card view

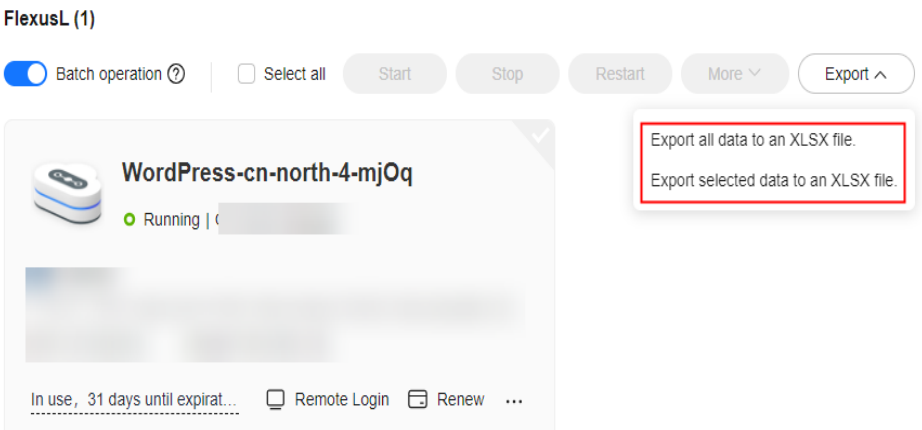
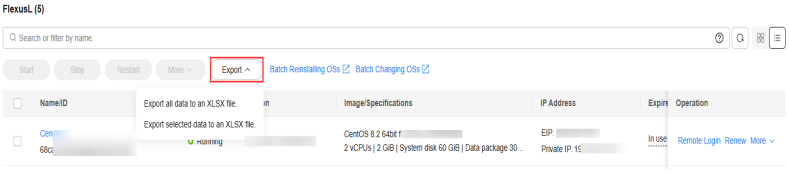


Figure 4-48 Export in the list view



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 the underlying OS (Ubuntu 22.04), application software, initialization data, and runtime environment required by the application. You can use application images to quickly deploy applications without upload and installation operations. For details about how to perform operations on the application image dashboard, see **Application Management (For Application Images Only)**.
Private Images	You can use a private image to quickly create a FlexusL instance with the same configuration as the image, or use a private image to change the OS. Private images are created from servers on cloud platforms or downloaded from third-party platforms. They can be used by FlexusL only after being created or imported using **Image Management Service (IMS)**.

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	16.04/18.04/20.04/22.04/24.04	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 **Application Management (For Application Images Only)**.

Image Name	Description
WordPress	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	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	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	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	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	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	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	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	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.
Kodbox	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. The Kodbox application image uses Ubuntu 22.04. It is deployed using Docker. The Kodbox application and the required operating environment have been preconfigured.
Node.js	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 Application Image Dashboard	You can log in to the visual dashboard of the application image for quick configuration.

Operation	Description
Best Practices for FlexusL	You can purchase application images for different scenarios as required and deploy applications according to the guide.
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 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 FlexusL instance.

Constraints

Table 5-1 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.

Item	Description
Image type	Only system disk private images are supported. Data disk private images and full-server private images are not supported. • Linux system disk images only support the following image sources: free 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.

NOTE

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 5-2 Creating or sharing an image using IMS

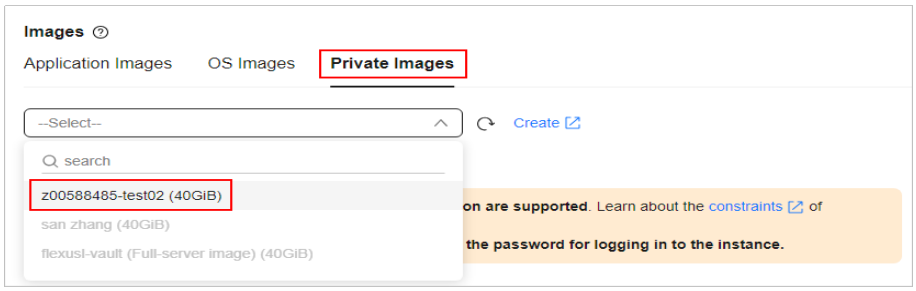
Image Source		Related Operations
Scenario 1	If your private image is created from a Huawei Cloud ECS or BMS, it can be used in the current region. If you want to use the private image in another region, replicate the image to the region where you want to use it first.	• **Creating a System Disk Image from an 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 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 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 image provider, 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 FlexusL 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 FlexusL Instance and I Know the Initial Password of the Private Image?**
- If you use a private image to create a FlexusL instance with Host Security (HSS) included, HSS will not protect the instance. You need to 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?**

6 Application Management (For Application Images Only)

FlexusL instances provide various featured application images. An application image contains the underlying OS (Ubuntu 22.04), application software, initialization data, and runtime environment required by the application. You can use application images to quickly deploy applications without upload and installation operations.

After creating a cloud server using an application image, you can manage the applications on the dashboard and O&M page provided by the application image.

- Dashboard: An application image provides a **visualized dashboard** where you can easily configure applications, such as managing software, plug-ins, and databases, after login.
- O&M page: The O&M page for application images is used to store initial passwords of dashboards, upload files, and configure domain names to provide O&M support for application deployment.

The differences between the login modes, initial usernames, and passwords of FlexusL instances, dashboard, and O&M page are listed in the following table.

Table 6-1 Differences between FlexusL instances, dashboard, and O&M page

Item	Login Mode	Initial Username and Password
FlexusL	Log in to the system through the console or other modes. For details, see **Login Modes**.	The default username of a Windows FlexusL instance is **Administrator**, and that of a Linux FlexusL instance is **root**. FlexusL instances do not have initial passwords. You need to **reset the passwords** on the FlexusL console.

Item	Login Mode	Initial Username and Password
Dashboard	Before logging in to an application dashboard for the first time, **initialize the application preinstalled in the image**. Then you can **log in to the application dashboard** on the FlexusL console.	The initial usernames and passwords of application dashboards vary depending on application images. For details, see **Best Practices for FlexusL**. • The dashboards of some application images, such as the WordPress application image, do not have initial usernames and passwords. You can set them during application initialization. • The dashboards of some application images, such as the Moodle application image, have initial usernames and passwords stored on the O&M page. • To obtain the initial usernames and passwords of dashboards of some application images such as the BT Panel application image, you need to log in to servers and run specific commands.
O&M page	In the address bar of a local browser, enter **http://*EIP*:9000** to log in to the application O&M page.	The username and password for logging in to the O&M page are the same as those for logging in to FlexusL instances.

Initializing an Application

During the initialization, you need to set the information about the application. Initialization operations vary depending on application images. **Table 6-2** lists the application images and their initialization operations.

Table 6-2 Application images and their initialization operations

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.

Logging In to the Application Dashboard

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. For details, see **Initialize Prestashop**.

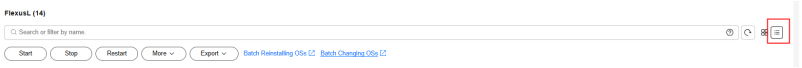
For application images other than Prestashop, perform the following steps to log in to the application dashboard:

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

   NOTE

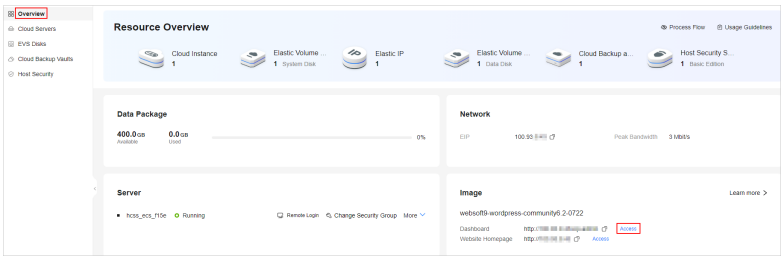
   By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

   Figure 6-1 Switching views

2. On the **Overview** page, in the **Image** area, click **Access** to access the application image dashboard.

   Figure 6-2 Accessing the dashboard

   The initial username and password for an application dashboard vary depending on the application images. Different application images support

different application management operations. For details, see **Best Practices for FlexusL** for the corresponding application images.

- The dashboards of some application images, such as the WordPress application image, do not have initial usernames and passwords. You can set them during application initialization.
- The dashboards of some application images, such as the Moodle application image, have initial usernames and passwords stored on the O&M page.
- To obtain the initial usernames and passwords of dashboards of some application images such as the BT Panel application image, you need to log in to servers and run specific commands.

Helpful Links

- **How Do I Check that an Application Image Has Been Up and Running?**
- **Why Cannot I Open the Dashboard of the Application Pre-installed in the Application Image?**
- **Why Cannot I Access the Dashboard of the Application Pre-installed in the Application Image After Entering the Initial Username and Password?**

7 Managing EVS Disks

7.1 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 will automatically attach the data disk to your 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.

7.2 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 do not need to purchase a system disk separately. **If you have additional storage requirements, you can add a data disk.**

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

This section describes how to add 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 the attached 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.

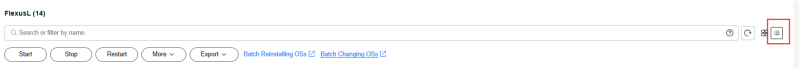
Procedure

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

   NOTE

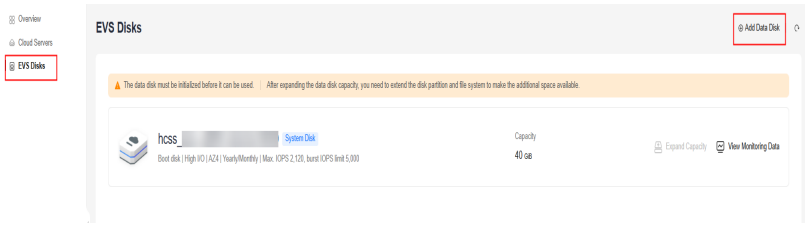
   By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

   Figure 7-1 Switching views

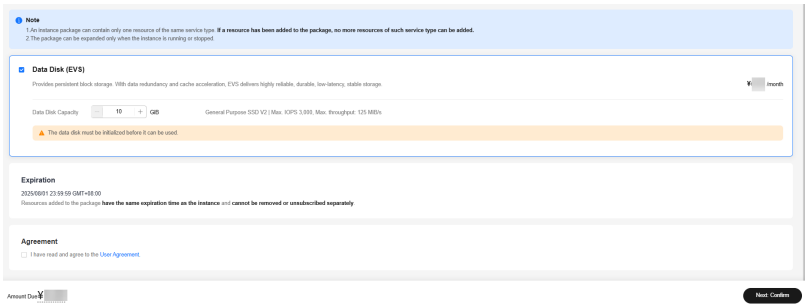
2. In the navigation pane on the left, choose **EVS Disks**. On the displayed page, click **Add Data Disk**.

   Figure 7-2 Adding a data disk

3. Select **Data Disk (EVS)** and set the data disk capacity.

   Figure 7-3 Configuring the data disk

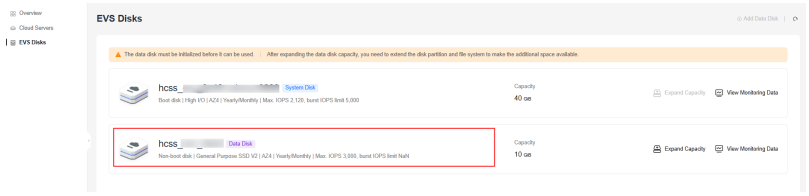
NOTE

- 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.

Figure 7-4 Checking the data disk



Helpful Links

- If the capacity of an existing data disk is insufficient, you can perform the operations in **Expanding Capacity of a Data Disk**.
- To ensure data security, you are advised to perform **Backing Up a FlexusL Instance** periodically.

7.3 Expanding Capacity of a Data Disk

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

Constraints

- 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**.
- 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.

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.

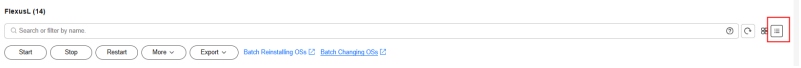
Step 1: Expand the Disk Capacity on the Console

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

   NOTE

   By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

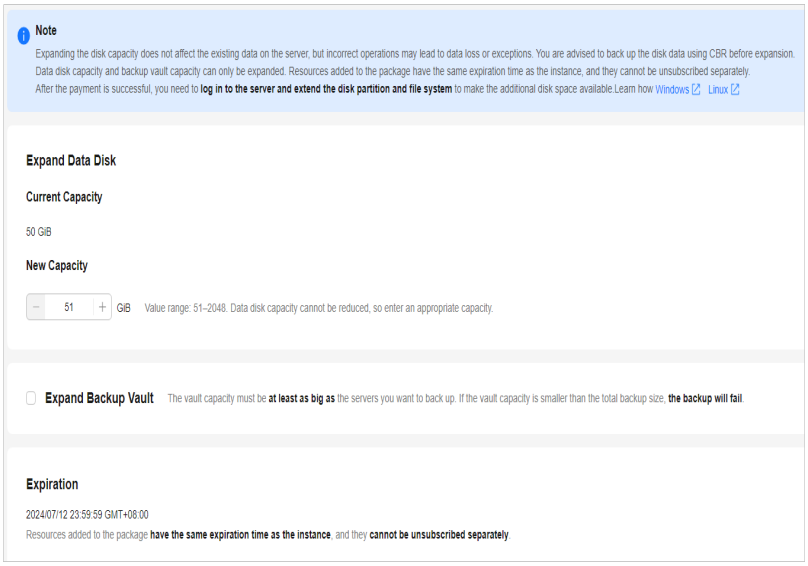
   Figure 7-5 Switching views

2. In the list on the left, choose **EVS Disks**. Then click **Expand Capacity**.
3. On the displayed page, enter a new capacity.

   If your FlexusL instance contains the cloud backup service, the **Expand Backup Vault** option will be available. Determine whether to expand the backup vault based on your requirements.

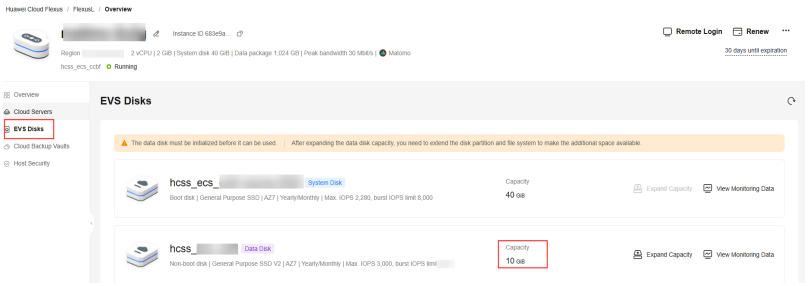
   - To expand the backup vault, select **Expand Backup Vault** and enter a new capacity.
   - To retain the vault capacity, ignore this configuration.



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

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

Figure 7-6 Checking the disk capacity



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)**.

8 Managing Server Security

8.1 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 8-1 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 8-2 lists some high-risk ports. Do not use these ports for your services.

Table 8-2 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

For details about security groups, see **Configuring the Security Group for a FlexusL Instance**.

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**.

8.2 Configuring the Security Group for a FlexusL Instance

8.2.1 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.

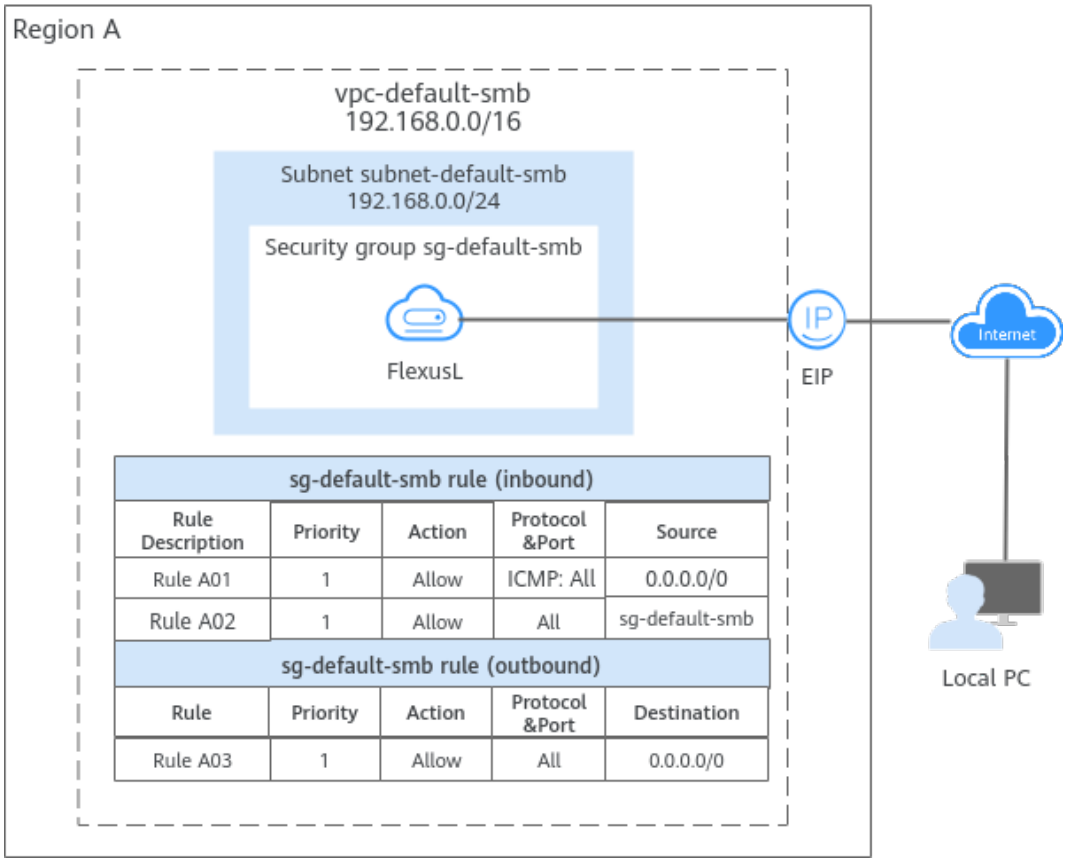
When you create a FlexusL instance, the system automatically creates a default security group (sg-default-smb) and associates it with the instance. You can also create a security group based on service requirements and associate it with the instance. An instance can be associated with multiple security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

Each security group can have both inbound and outbound rules. You need to specify the source, port, and protocol for each inbound rule and specify the destination, port, and protocol for each outbound rule to control the inbound and outbound traffic to and from the instances in the security group. **Figure 8-1** shows an example of a security group architecture. In region A, after a FlexusL instance is created, it is automatically associated with the default VPC vpc-default-smb and subnet subnet-default-smb. The FlexusL instance is also associated with the default security group sg-default-smb in subnet-default-smb to ensure the network safety for the FlexusL instance.

- Security group sg-default-smb has a custom inbound rule to allow ICMP traffic to the FlexusL instance from your PC over all ports. However, the security group does not contain a rule to allow external access to the instance over the SSH port 22 or RDP port 3389. As a result, you cannot remotely log in to the FlexusL instance from your PC.

- If the FlexusL instance needs to access the Internet through an EIP, the outbound rule of sg-default-smb must allow all traffic from the FlexusL instance to the Internet.

Figure 8-1 A security group architecture



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.

You can specify a protocol, port, source or destination for a security group rule. The following describes key information about a security group.

Table 8-3 Key parameters of a security group rule

Parameter	Description
Priority	The value ranges from 1 to 100. A smaller value indicates a higher priority. Security group rules are matched by priority and then by action. Deny rules take precedence over allow rules.

Parameter	Description
Action	**Allow** or **Deny**. If the protocol, port, source or destination of the traffic matches a security group rule, traffic will be allowed or denied.
Type	IPv4 or IPv6.
Protocol & Port	Network protocol type and port range. • Network protocol: the protocol that is used to match traffic. The protocol can be TCP, UDP, ICMP, or GRE. • Port range: the destination port that is used to match traffic. The value ranges from 1 to 65535.
Source or Destination	Source address of traffic in the inbound direction or destination address of traffic in the outbound direction. The source or destination can be an IP address, security group, or IP address group. • IP address: a fixed IPv4/IPv6 address or IPv4/IPv6 CIDR block, for example, 192.168.10.10/32 (IPv4 address), 192.168.1.0/24 (IPv4 CIDR block), or 2407:c080:802:469::/64 (IPv6 CIDR block). • Security group: If the selected security group and the current security group are in the same region, the traffic is allowed or denied to the private IP addresses of all instances in the selected security group. For example, if there is instance A in security group A and instance B in security group B, and the inbound rule of security group A allows traffic from security group B, traffic is allowed from instance B to instance A. • IP address group: If you have multiple IP addresses with the same security requirements, you can add them to an IP address group and select this IP address group when you configure a rule, to help you manage them in an easier way.

By default, the inbound rules of FlexusL default security group sg-default-smb only allow instances in the same security group to communicate with each other and deny all external requests. The security group outbound rules enable all ports and allow all requests that originate from the instances in the security group. Each security group has default rules. For details, see **Table 8-4**. You can also customize security group rules. For details, see **Configuring Security Group Rules for a FlexusL Instance**.

Table 8-4 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.

NOTE

If the source is set to 0.0.0.0/0 or ::/0, all external IP addresses are either allowed or denied to access your instances, depending on if the action is Allow or Deny. If the access is allowed, exposing high-risk ports, such as port 22, 3389, or 8848, to the public network will leave your instances vulnerable to network intrusions, service interruptions, data leakage, or ransomware attacks. You should only configure known IP addresses for the source in security group rules.

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.

Reference

- **Configuring Security Group Rules for a FlexusL Instance**
- **Changing the Security Group of a FlexusL Instance**
- **Configuring Security Groups for FlexusL Application Images**

8.2.2 Configuring Security Group Rules for a FlexusL Instance

Scenarios

A security group is a collection of access control rules and 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.
- Add as fewer rules as possible. 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.

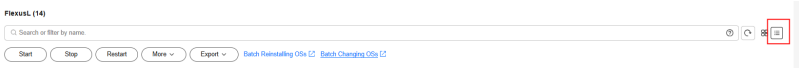
Procedure

1. Log in to the FlexusL **console**.
2. Configure security group rules using any of the following methods:

   NOTE

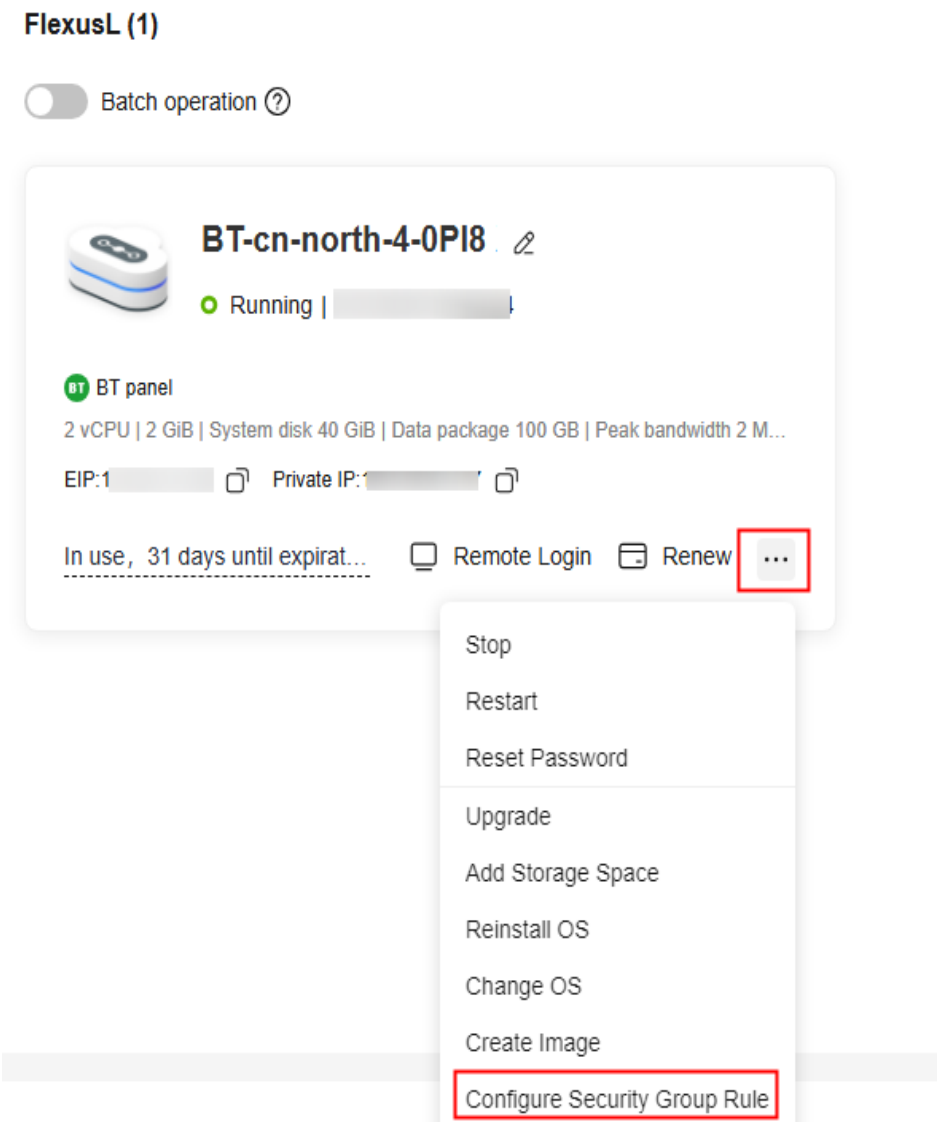
   By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

   Figure 8-2 Switching views

- Method 1: In the card view, locate the target resource card and choose ··· > **Configure Security Group Rule**.

  Figure 8-3 Configuring security group rules from the resource card

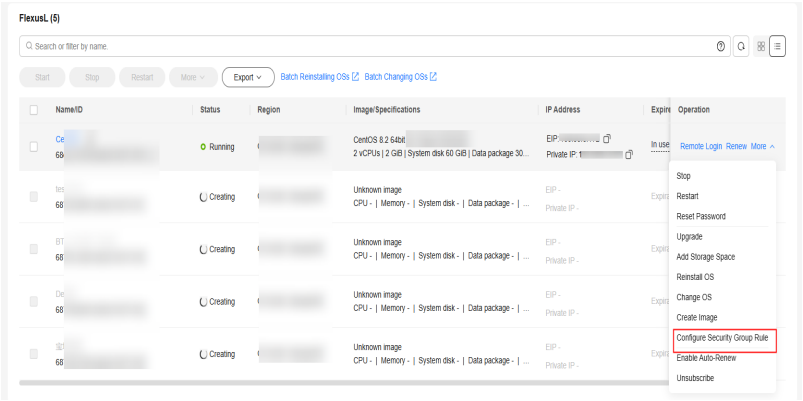
  

  NOTE

  This configuration is unavailable on the HA package resource card.

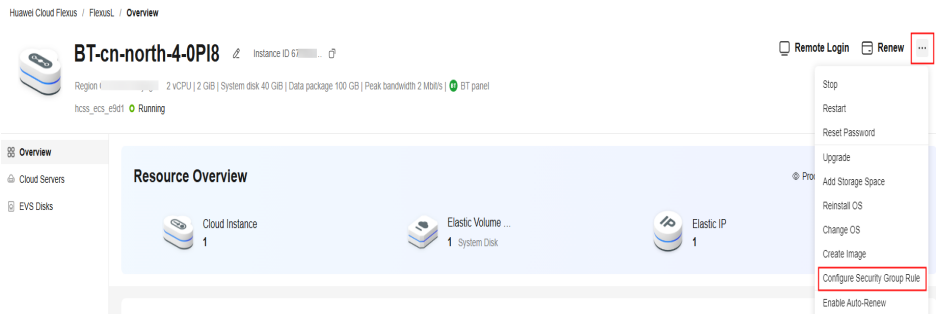
- Method 2: In the list view, locate the target FlexusL instance and choose **More** > **Configure Security Group Rule** in the **Operation** column.

Figure 8-4 Configuring security group rules from the list page



– Method 3: On the resource details page, choose > **Configure Security Group Rule** in the upper right corner.

Figure 8-5 Configuring security group rules from the resource details page



NOTE

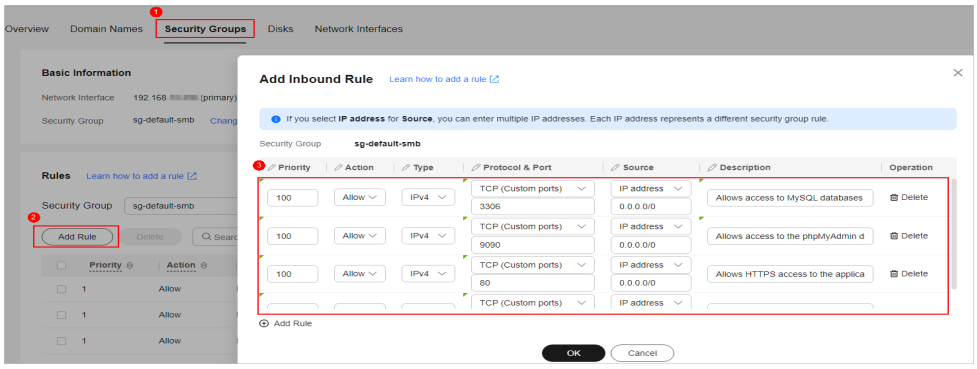
This configuration is unavailable on the overview page of HA package resource card.

– Method 4: On the resource details page, choose **Cloud Servers** from the left navigation pane. Click the cloud server name and then click the **Security Groups** tab.

3. Select **Inbound rules** from the drop-down list and click **Add Rule**.

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

Figure 8-6 Adding an inbound rule



4. Select **Outbound rules** from the drop-down list and click **Add Rule**.

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

5. Click **OK**.

   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**.

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.

Reference

- **Configuring Security Groups for FlexusL Application Images**
- **Why Are My Security Group Rules Not Working?**

8.2.3 Changing the Security Group of a FlexusL Instance

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

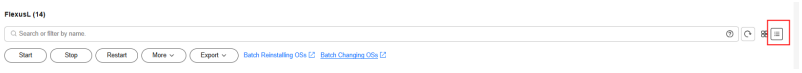
Modifying a Security Group

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

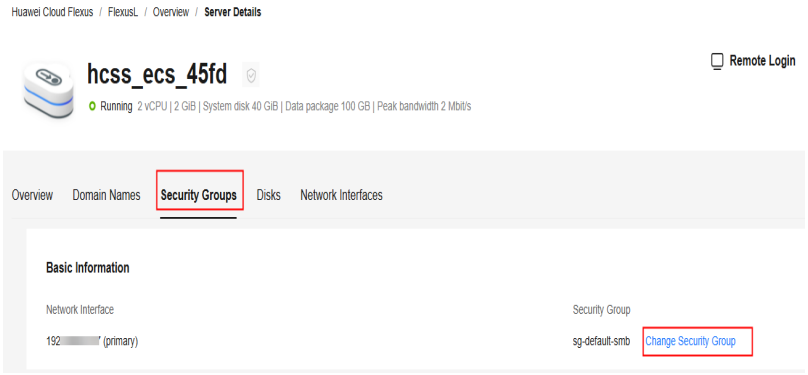
NOTE

By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

Figure 8-7 Switching views



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**.

8.2.4 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 8-5 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: 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 8-6 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: 3306	0.0.0.0/0	Allows access to MySQL databases.
1	Allow	IPv4	TCP: 9090	0.0.0.0/0	Allows access to the phpMyAdmin database management tool.
1	Allow	IPv4	TCP: 8888	0.0.0.0/0	Allows access to the BT panel dashboard.
1	Allow	IPv4	TCP: 443	0.0.0.0/0	Allows access to the FlexusL instance via HTTPS.
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Allows access over HTTP.

Matomo, Odoo, Nextcloud, and GitLab

Table 8-7 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: 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 8-8 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 22	0.0.0.0/0	Allows access to the FlexusL instance using SSH locally.
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of application images.
1	Allow	IPv4	TCP: 3306	0.0.0.0/0	Allows access to MySQL databases.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.
1	Allow	IPv4	TCP: 9000	0.0.0.0/0	Allows external access to the application O&M page.

SRS

Table 8-9 Security group rules

Priority	Action	Type	Protocol & Port	Source	Description
1	Allow	IPv4	TCP: 22	0.0.0.0/0	Allows access to the FlexusL instance using SSH locally.
1	Allow	IPv4	TCP: 80	0.0.0.0/0	Specifies the internal forwarding port of application images.
1	Allow	IPv4	TCP: 9001	0.0.0.0/0	Allows external access to the application dashboard.
1	Allow	IPv4	TCP: 1935	0.0.0.0/0	Allows access to the RTMP livestreaming server.
1	Allow	IPv4	TCP: 1985	0.0.0.0/0	Allows access to the HTTP API server to deliver HTTP-API and WebRTC streams.
1	Allow	IPv4	TCP: 8080	0.0.0.0/0	Allows access to the HTTP livestreaming server to deliver HTTP-FLV and HLS streams.
1	Allow	IPv4	TCP: 8000	0.0.0.0/0	Allows access to the WebRTC media server.

8.3 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.

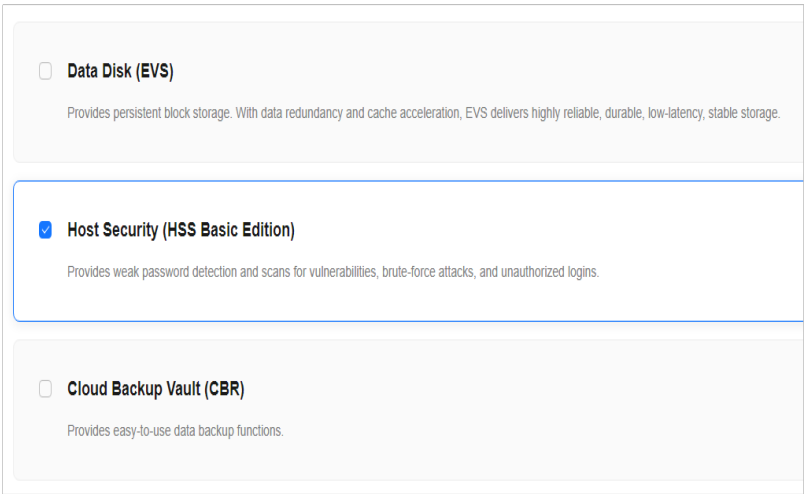
For more information about HSS, see **What Is HSS?**

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 8-8 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 8-10 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 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

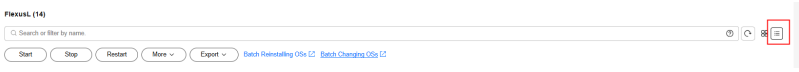
To view detection details about HSS enabled during the FlexusL instance purchase, perform the following steps. To view detection details about HSS that is not enabled during the FlexusL instance purchase, see **Viewing Detection Details**.

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

   NOTE

   By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

   Figure 8-9 Switching views

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 **Enabled**. When the FlexusL instance expires, HSS stops protecting the instance server. • **Enabled**: The server is fully protected by HSS. • **Unprotected**: HSS is disabled for the server. The Agent may fail to be installed. For details, see **Viewing Server Protection Status** to check the Agent status and follow the instructions to install the Agent. • **Protection interrupted**: The server is not protected, because the HSS protection server is interrupted. The protection may be interrupted because the server is stopped, or the Agent is offline or uninstalled. For details, see **Viewing Server Protection Status** to view the Agent status and interruption cause.
Server status	Status of the server You can click **View protected server** to go to the cloud server overview page.
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

9 Managing Backups

9.1 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 9-1 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 to 10,485,760, in GiB	More flexible

Constraints

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

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

9.2 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

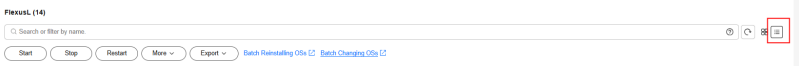
After you associate a cloud backup vault with a FlexusL instance server during the purchase, the cloud server can be automatically backed up based on the policy. You can view or modify the backup policy on the FlexusL console.

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

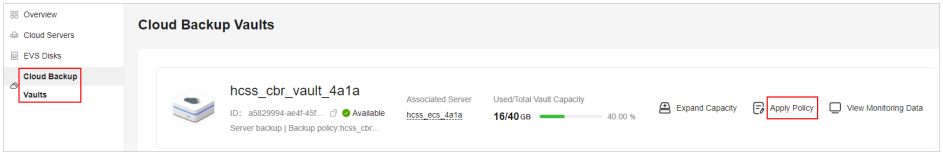
   NOTE

   By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

   Figure 9-1 Switching views

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.

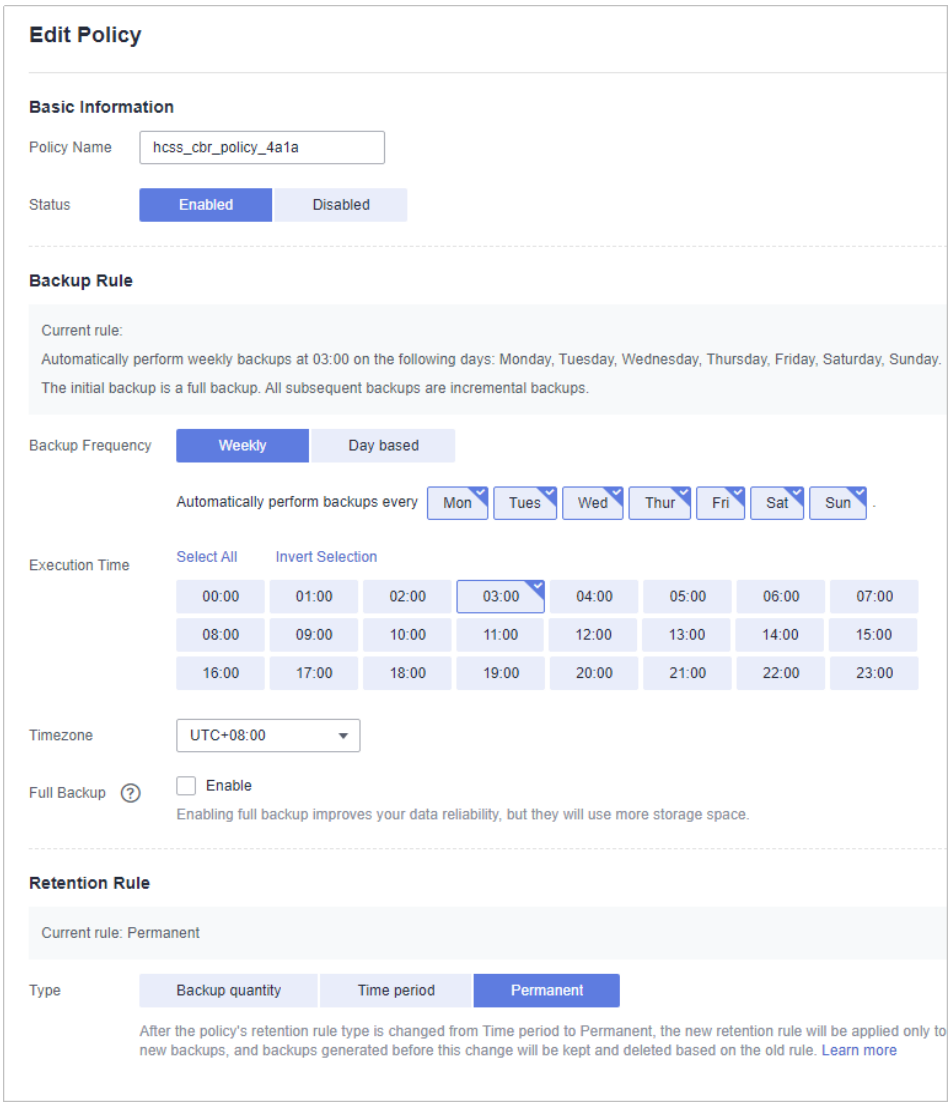


3. View or set the backup policy parameters.

   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.

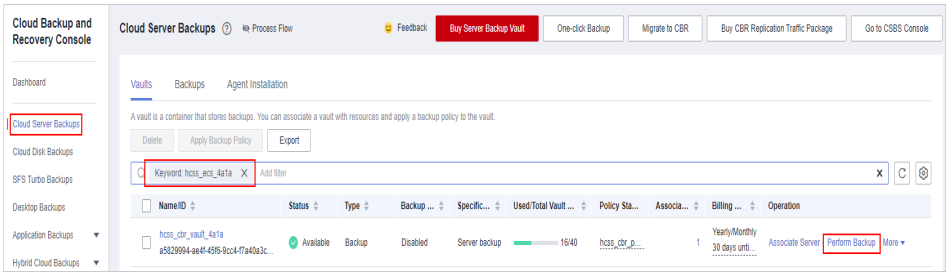
Method 2: Manual Backup

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.

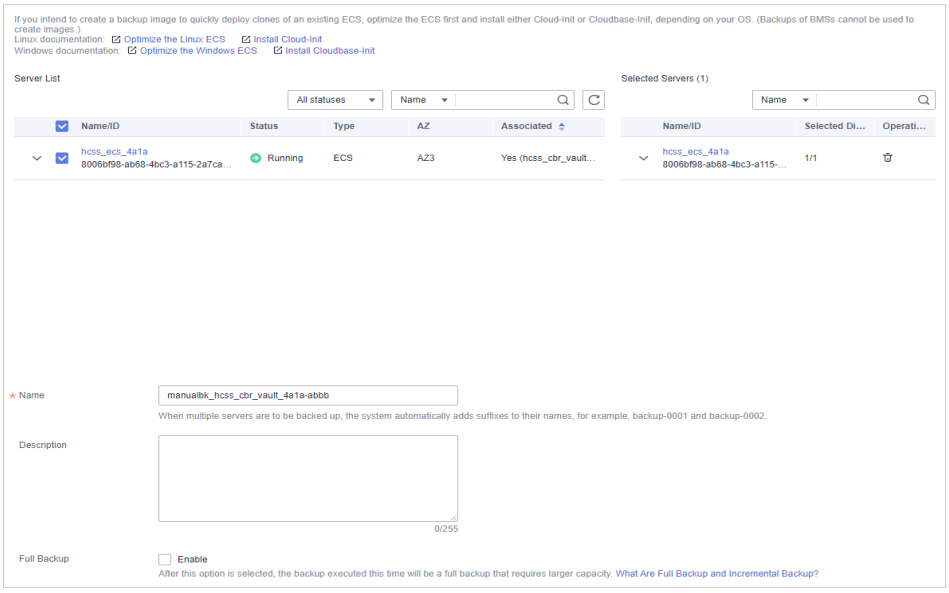
     

   - If you associate a vault with a FlexusL instance server on the CBR console after the FlexusL instance is created, search by server ID.
2. Log in to the **CBR console** and choose **Cloud Server Backups**. On the **Vaults** tab in the right pane, search for the vault using the obtained vault name or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

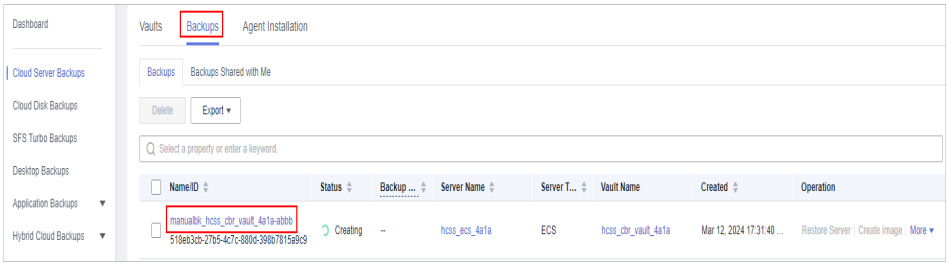
3. Set a backup name and determine whether to enable **Full Backup**.

   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**.

9.3 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. For details about the FlexusL backup pricing, see **FlexusL Price Calculator**.

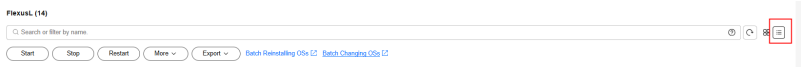
Procedure

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

   NOTE

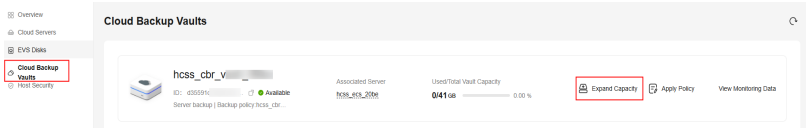
   By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

   Figure 9-2 Switching views

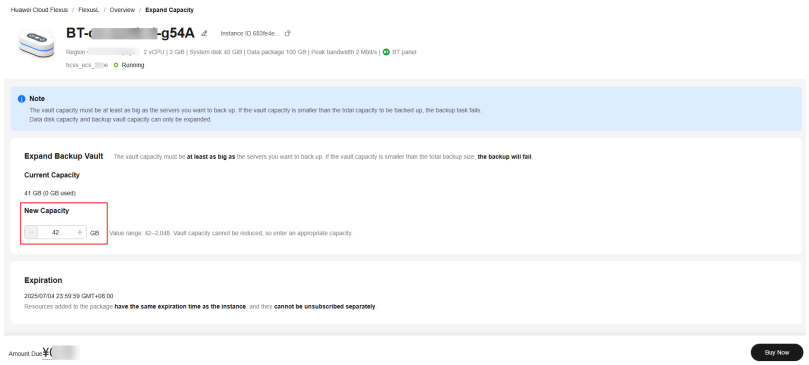
2. Choose **Cloud Backup Vaults** and click **Expand Capacity**.

   Figure 9-3 Expanding vault capacity

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

   Figure 9-4 Configuring the capacity to be expanded

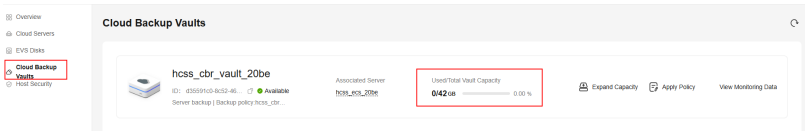
   

   The vault capacity must be at least as big as the server capacity you want to back up. If the vault capacity is smaller than the total capacity to be backed up, the backup task will fail. For example, if your system disk and data disks use 80 GiB, the vault capacity must be greater than 80 GiB. Otherwise, the backup will fail.

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

   After the purchase, wait until the FlexusL status changes to **Running** again. Then, check whether the expanded cloud backup capacity is normal.

Figure 9-5 Checking the capacity after expansion



10 Adding and Resolving a Domain Name for a FlexusL Instance

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. This section describes how to add a domain name and configure DNS for a FlexusL instance.

What Are a Domain Name and DNS Resolution?

A domain name is a name entered in the address box of a web browser, for example, **example.com**, to access a website or web application.

Domain registration is a service that you need to pay for the use of a domain name on the Internet for a period of time.

DNS resolution translates a domain name (for example, www.example.com) and its subdomains into IP addresses like 192.1.2.3. For details, see **What Is DNS?**

Before creating a service on Internet, register a domain name. In the Internet, a domain name corresponds to an IP address. After you enter a domain name in the browser, the DNS server will resolve your domain name into an IP address so that Internet requests can be routed to the corresponding servers using the IP address and get responds.

What Is an ICP Filing?

An Internet Content Provider (ICP) filing is a legal requirement in the Chinese mainland. All websites based in the Chinese mainland must complete an ICP filing. Anyone who does not obtain an ICP file or license cannot provide non-commercial or commercial Internet information services.

An ICP filing is required for both your website server and domain name. You need to apply for ICP licensing after the domain name is registered and the website is set up. If the website is not licensed, the web browser cannot access the website using the obtained IP address.

For details, see **What Is an ICP Filing?**

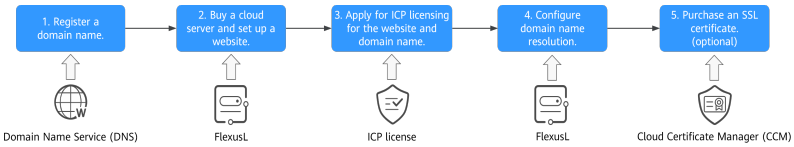
What Is an SSL Certificate?

An SSL certificate is an SSL-compliant digital certificate issued by a trusted CA.

After an SSL certificate is deployed on a server, HTTPS is enabled on the server. The server uses HTTPS to establish encrypted links to the client, ensuring data transmission security. For details, see **What Is Cloud Certificate Manager?**

Process of Accessing a Website Using a Domain Name

Figure 10-1 Process of accessing a website through a domain name



1. Register a domain name.

   Register the domain name with a domain name registrar.

2. Purchase a cloud server and set up a website.

   Select and purchase a FlexusL instance and deploy a website or application based on your service requirements. For details, see **Purchasing a FlexusL Instance** and **Best Practices for Using FlexusL**.

   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).

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. Huawei Cloud provides you with free ICP licensing services. For details, see **ICP Filing Process**.

4. Configure domain name resolution.

   You can add and resolve a domain name on the FlexusL console. Website services can be provided only after the added domain name is resolved successfully. For details, see **Adding and Resolving a Domain Name for a FlexusL Instance**.

5. (Optional) Purchase an SSL certificate.

   To use HTTPS, **purchase and install an SSL certificate** for the instance. After the certificate is installed, you can access the website using **https://** *<associated_domain_name>*.

Precautions

- A non-registered domain name can be added, but it must be registered and licensed afterwards. Otherwise, it cannot be used to access the website. To ensure that a domain name can be used normally, register it and complete ICP licensing before adding the domain name. For details, see **Process of Accessing a Website Using a Domain Name**.

- Before resolving a domain name, check whether the domain name has expired or is abnormal. Expired or abnormal domain names cannot be resolved.
- Before a domain name is resolved, 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.

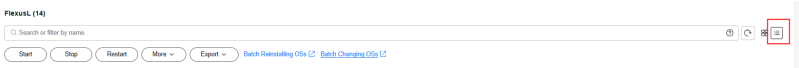
Adding and Resolving a Domain Name for a FlexusL Instance

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

   NOTE

   By default, the FlexusL console is displayed in card view. You can switch to the list view as needed.

   Figure 10-2 Switching views

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. Add a domain name using one of the following methods based on the site requirements.
   - Enter a domain name.

     Configure the domain name and click **OK**.

     Figure 10-3 Adding a domain name

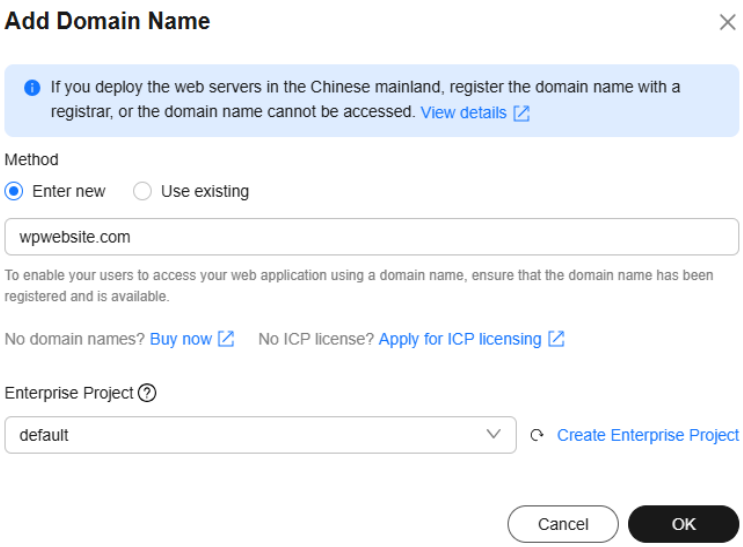
     

Table 10-1 Domain name parameters

Parameter	Description
Method: Enter new	Enter a domain name to be added for the instance, for example, wpwebsite.com.
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.

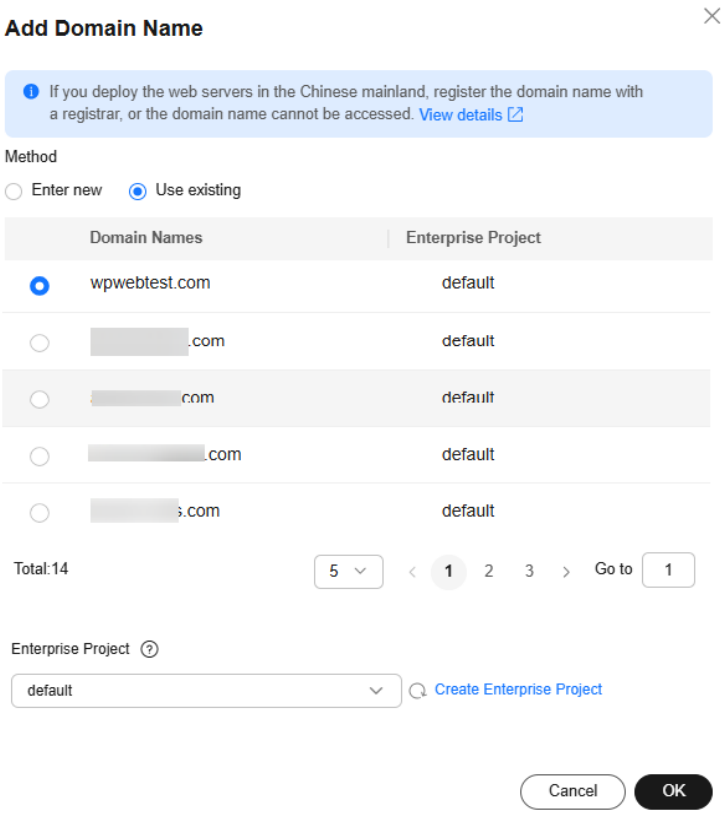
- Use an existing domain name.

  Select the domain name to be added from the list, select an enterprise project as required, and click **OK**.

  NOTE

  This parameter is displayed only when your account is an enterprise account.

Figure 10-4 Using an existing domain name



5. In the **Configure Record Set** dialog box, set the following parameters to resolve the domain name or subdomain name to the EIP, of the current server and click **OK**.

If you do not need to resolve the domain name now, click **Cancel**. You can click **Configure Record Set** in the **Operation** column of the domain name later.

Figure 10-5 Resolving a domain name

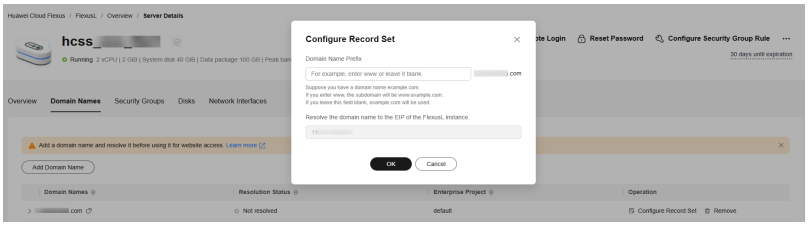


Table 10-2 Resolving a domain name

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.

6. (Optional) Change the DNS server addresses.

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

   - 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**.

7. View the added domain name in the domain name list.

Figure 10-6 Domain names

Table 10-3 Domain names

Parameter	Description
Domain Names	Domain name added to the FlexusL instance.
Resolution Status	Whether the resolution is complete. • Resolved • Not resolved
Enterprise Project	Enterprise project associated with the domain name.
Operation	• Configure Record Set If you need to add more domain name resolution records, click **Configure Record Set** and resolve the domain name or subdomain name to the EIP of the current FlexusL as prompted. For details about the parameters, see **Table 10-2**. • Remove 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.

8. Click ⌄ on the left of the domain name to view the resolved domain name.

Figure 10-7 Resolved domain names

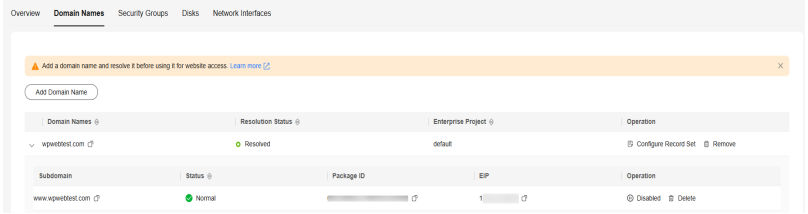


Table 10-4 Resolved domain names

Parameter	Description
Subdomain	Resolved domain name.
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

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

Helpful Links

- **How Do I Check Whether a Record Set Has Taken Effect?**
- **What Do I Do If a Record Set Does Not Take Effect?**

11 Monitoring FlexusL Instances Using Cloud Eye

11.1 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.

For details, see **Viewing Monitoring Metrics of a FlexusL Instance**.

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 11-2**.
- 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.

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.

11.2 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 FlexusL instances restart or recover, 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.

Viewing Common Monitoring Metrics

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

   Alternatively, enter the instance name, EIP, or server ID in the search box to filter the target FlexusL instance.
3. On the **Overview** page, view the common monitoring metrics in the **Data Monitoring** area. For details, see **Table 11-1**.

- You can view the data curves of the last 15 minutes, last 30 minutes, last 1 hour, last 2 hours, last 3 hours, last 12 hours, and last 24 hours.
- You can select a metric value type, including **Raw Value**, **Average Value**, **Max.**, **Min.**, and **Sum**.

- **Raw Value** is the metric data that is not processed or converted.
- **Average Value** is the value calculated by averaging raw data over a rollup period.
- **Max.** is the highest value observed during a rollup period.
- **Min.** is the lowest value observed during a rollup period.
- **Sum** is the sum of raw data during a rollup period.

Rollup is a process where Cloud Eye calculates the maximum, minimum, average, or sum value of raw data sampled for different periods and repeats the process for each subsequent period. Each period is called a rollup period. A rollup period can be 1 minute, 5 minutes, 20 minutes, and 1 hour. Select a rollup period based on your service requirements.

- You can click the refresh icon or enable **Auto Refresh** to refresh the page. If **Auto Refresh** is enabled, the page is automatically refreshed every 30 seconds.

Figure 11-1 Common monitoring metrics of FlexusL instances

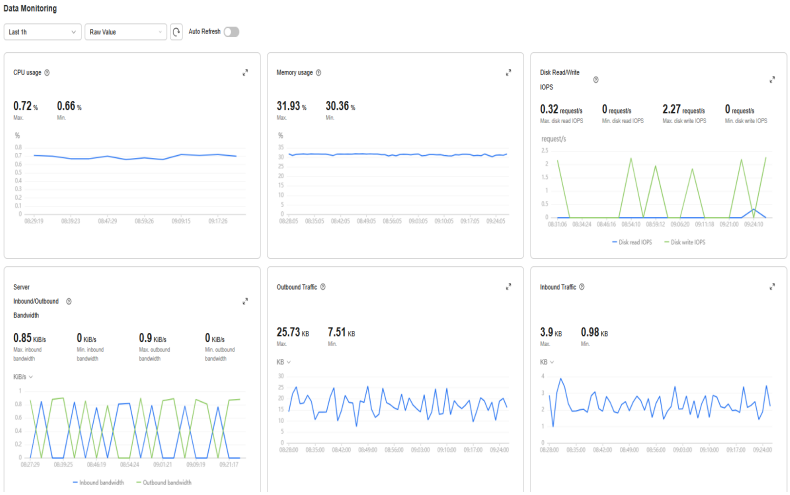


Table 11-1 Common monitoring metrics

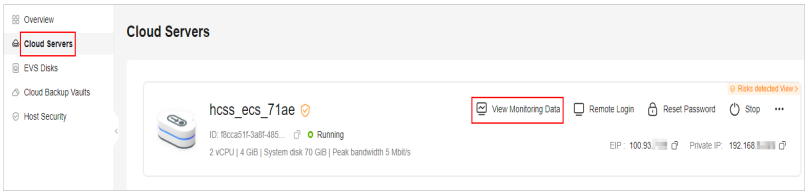
Metric	Description
CPU Usage	CPU usage of the physical server accommodating the monitored cloud server, which is not as accurate as that obtained from the cloud server that is being monitored
Memory Usage	The amount of memory that is available and can be given instantly to processes
Disk Read/ Write IOPS	The number of read or write requests sent to the monitored disk per second
Server Inbound/ Outbound Bandwidth	The number of public and private bytes received or sent by the cloud server per second
Inbound Traffic	The amount of data coming into a cloud server

Metric	Description
Outbound Traffic	The amount of data coming out of a cloud server

Viewing All Monitoring Metrics

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

   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 data curves of the last 15 minutes, last 30 minutes, last hour, last 2 hours, last 3 hours, last 12 hours, last 24 hours, last 7 days, last 30 days, or a custom time range.
   - You can select a metric value type, including **Raw Value**, **Average Value**, **Max.**, **Min.**, and **Sum**.
     - **Raw Value** is the metric data that is not processed or converted.
     - **Average Value** is the value calculated by averaging raw data over a rollup period.
     - **Max.** is the highest value observed during a rollup period.
     - **Min.** is the lowest value observed during a rollup period.
     - **Sum** is the sum of raw data during a rollup period.

     Rollup is a process where Cloud Eye calculates the maximum, minimum, average, or sum value of raw data sampled for different periods and repeats the process for each subsequent period. Each period is called a rollup period. A rollup period can be 1 minute, 5 minutes, 20 minutes, and 1 hour. Select a rollup period based on your service requirements.
   - 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 zoom in the graph.

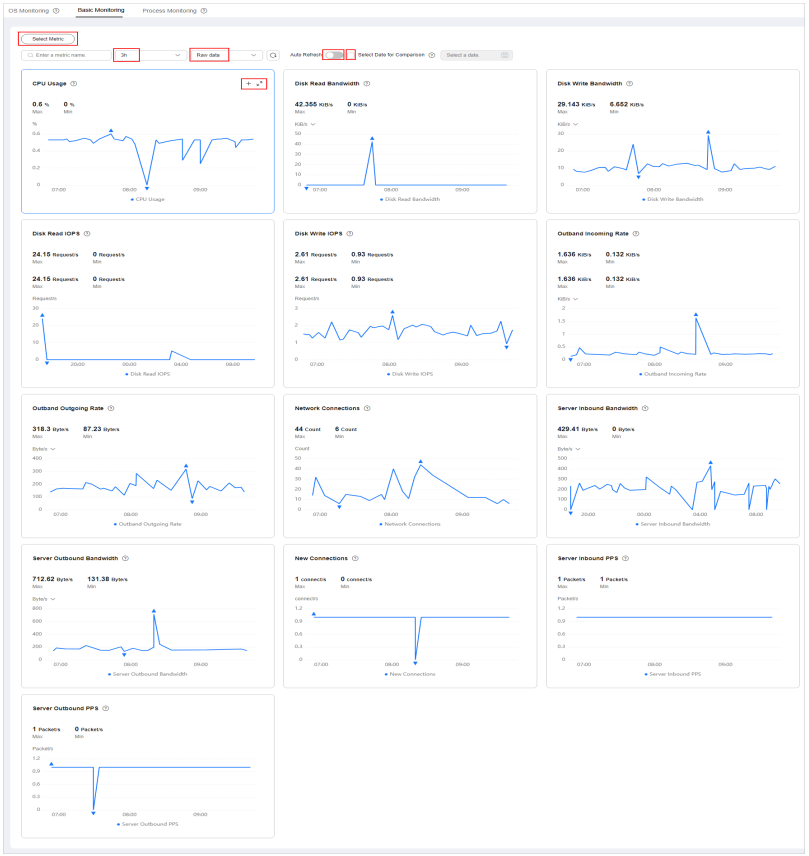


Table 11-2 Basic monitoring metrics

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

Metric	Description
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
Network Connections	Total number of TCP and UDP connections on a cloud server Unit: N/A
Server Inbound Bandwidth	Number of public and private bytes received by the cloud server per second Unit: Byte/s
Server Outbound Bandwidth	Number of public and private bytes sent by the cloud server per second Unit: Byte/s
Server Inbound PPS	Number of public and private packets received by the cloud server per second Unit: Packet/s

Metric	Description
Server Outbound PPS	Number of public and private packets sent by the cloud server per second Unit: Packet/s
New Connections	Number of new connections (including TCP, UDP, and ICMP) created on the cloud server Unit: N/A

