Flexus X Instance

User Guide

Issue	01
Date	2025-10-27

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 Using IAM to Grant Access to FlexusX

FlexusX allows you to use **IAM** to implement fine-grained permissions control on your FlexusX 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 FlexusX 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 FlexusX resources.

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

This section describes how to grant permissions to a FlexusX instance.

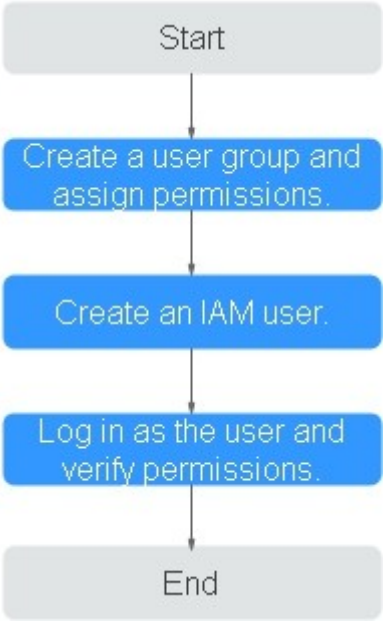
Creating a User and Granting Permissions for FlexusX Instances

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

The system-defined policies of a FlexusX instance are the same as those of an ECS.

- For details, see **Permissions Management**.
- **Figure 1-1** shows the process of creating a user and granting permissions for FlexusX instances. For details, see **Creating a User and Granting ECS Permissions**.

Figure 1-1 Process for granting FlexusX instance permissions.



Example Custom policies

You can create custom policies to supplement the system-defined policies of FlexusX. Custom policies of a FlexusX instance are the same as those of an ECS. For details, see **ECS Custom Policies**.

2 Purchasing a FlexusX Instance

Scenarios

When purchasing a FlexusX instance, you need to configure the instance specifications, image, storage, network, and security group. After the purchase is successful, you can use the FlexusX instance just like using a local PC or physical server.

This section describes how to purchase FlexusX instances on the management console.

Procedure

Step	Description
Preparations	Register a HUAWEI ID and enable Huawei Cloud services.
Step 1: Access the Page for Purchasing FlexusX Instances	Access the **Buy FlexusX Instance** page.
Step 2: Configure Parameters	Configure parameters based on your service requirements.
Step 3: Confirm the Configuration and Submit the Order	Confirm the configuration details and complete the purchase.

Preparations

Before creating 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**.

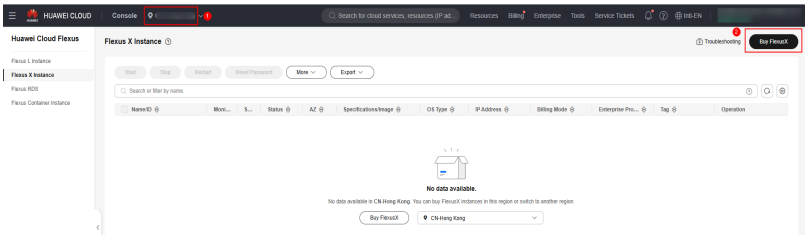
Real-name authentication is required only when you buy or use cloud services provisioned in the Chinese mainland.

Before purchasing a FlexusX instance, you need to understand the notes and constraints. For details, see **Notes and Constraints**.

Step 1: Access the Page for Purchasing FlexusX Instances

1. Log in to the FlexusX **console**. In the upper left corner, click  and select a region.
2. Click **Buy FlexusX**.

Figure 2-1 FlexusX instance page



Step 2: Configure Parameters

Configure required parameters for purchasing a FlexusX instance based on your service requirements.

Basic Configuration

Figure 2-2 Basic configurations for purchasing a FlexusX instance

Table 2-1 Basic configurations for purchasing a FlexusX instance

Parameter	Description
Billing Mode	FlexusX instances can be billed on a yearly/monthly or pay-per-use basis. For details, see **Billing**. • **Yearly/Monthly**: You can select a required duration and pay for the subscription in a single payment. • **Pay-per-use**: You do not need to select a required duration. Instead, you will be billed based on how long you use the instance.

Parameter	Description
Region	A region refers to a physical data center area where FlexusX instances reside. Select a region close to your services to reduce network latency and improve access speed. For services that need to communicate with existing cloud services through a private network, select the region where the existing cloud services are deployed. Exercise caution when selecting a region. Once a FlexusX instance is created, the region cannot be changed.
AZ	An AZ is a physical region where resources use independent power supply and networks. AZs are physically isolated but interconnected through an internal network. • Random • Specified an AZ.

Instance Specifications

Figure 2-3 Custom instance specifications

Table 2-2 Instance specifications parameters

Parameter	Description
Compute Type	x86: The compute is provided by x86 CPUs.
Performance Mode	FlexusX supports **the performance mode**. The performance mode can provide ultimate, stable performance assurance at additional costs. For details about the differences between performance and non-performance modes, see **Instance Specifications**.
Instance Specifications	You can select either preset or custom FlexusX instance specifications as needed. For more information about specifications, see **Instance Specifications**.

Image

Figure 2-4 Setting image information

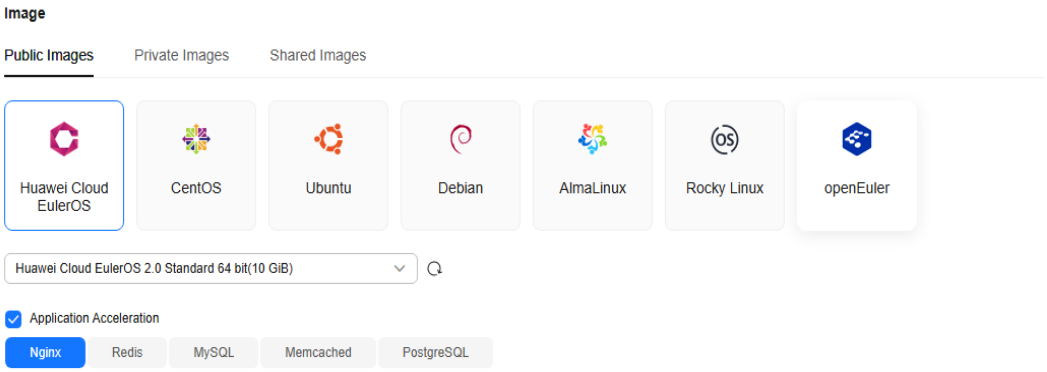


Table 2-3 Parameters for configuring images

Parameter	Description
Public Images	Public images are standard, widely used images. A public image contains an OS and pre-installed public applications. After your instance is created using a public image, you can deploy applications or software on the instance as required. **NOTE** • FlexusX instances that use the Huawei Cloud EulerOS 2.0 public image support application acceleration for Nginx, Redis, or MySQL, PostgreSQL or Memcached. For more information, see **Configuring Application Acceleration for a FlexusX Instance**.
Private images	Private images are created on **Image Management Service (IMS)**. You can create a private image from a cloud server on Huawei Cloud or another cloud platform, or you can download a third-party image. Before selecting a private image, you are advised to learn about the usage and constraints of private images described in **Creating a FlexusX Instance from a Private Image or Using a Private Image to Change the OS**. **NOTE** The FlexusX instance you are creating and the private image you want to select must belong to the same region. Otherwise, the image cannot be selected for the FlexusX instance. For example, if you want to create a FlexusX instance in the CN-Hong Kong region, you can only select images from the CN-Hong Kong region. If you want to use an image from another region, replicate that image to the current region. For details, see **Replicating Images Across Regions**.
Shared images	A shared image is a private image shared by another user.

Storage

Figure 2-5 Parameters for configuring storage devices

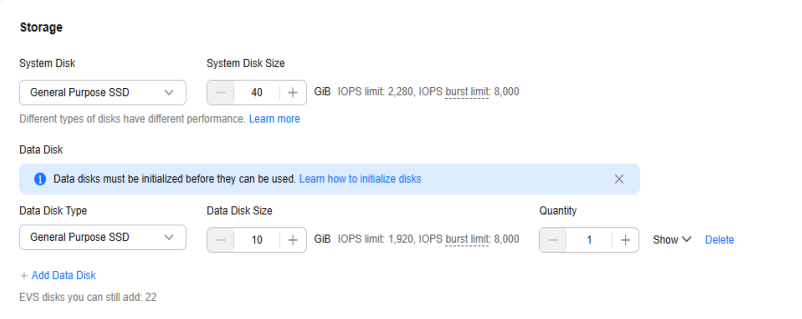


Table 2-4 Parameters for configuring storage devices

Parameter	Description
System Disk	Set the system disk type and size. Different disks have different performance. For details, see **EVS Concepts**. If the private image you selected is not encrypted, the system disk will not be encrypted, either. If the image you selected is encrypted, the system disk will be encrypted automatically.
Data Disk	Set the data disk type, size, and quantity. Click **Show** on the right of a data disk to set the following parameters if required: • **SCSI**: If you select this option, the device type of the data disk is SCSI. For more information about SCSI disks and supported FlexusX instances, see **Device Types**. • **Share**: If you select this option, the data disk is sharable. Such a disk can be attached to multiple FlexusX instances.

Network

Figure 2-6 Network parameters.

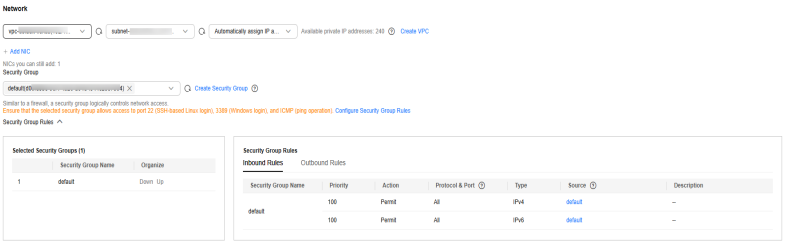


Table 2-5 Network parameters.

Parameter	Description
VPC	Select an available VPC and subnet from the drop-down list and specify how a private IP address will be assigned. • **Automatically assign IP address**: The system automatically assigns a private IPv4 address to the primary NIC. • **Manually specify IP address**: You need to manually assign a private IPv4 address to the primary NIC. Before specifying an IP address, click **View In-Use IP Address** to avoid address conflict. • **Use existing network interface**: This parameter is displayed only when the selected VPC has available network interfaces. You can select an existing network interface from the drop-down list as the primary network interface.
NIC	Click **Add NIC** to add multiple extension NICs and specify IP addresses for them (including primary NICs). If you specify an IP address and create multiple FlexusX instances in a batch, this IP address is the start IP address. Ensure that the IP address is consecutive, available within the specified subnet. The subnet that contains the specified IP address cannot overlap with other subnets.

Parameter	Description
IPv6	This parameter is available only if FlexusX instances are of specific flavors and in a VPC with IPv6 enabled. • IPv6 not required • Automatically-assigned IPv6 For details about how to enable IPv6 on a subnet, see **IPv4 and IPv6 Dual-Stack Network**. For details about how to check whether a FlexusX instance supports IPv4 and IPv6 dual stack, see "Constraints" in **Dynamically Assigning IPv6 Addresses**. By default, the system assigns IPv4 addresses. If you select **Automatically-assigned IPv6 address**, the system assigns IPv6 addresses. In a VPC, a FlexusX instance uses an IPv6 address to access the dual-stack intranet. To access the Internet, you must enable **IPv6 Bandwidth** and select a shared bandwidth. The FlexusX instance then can access the IPv6 Internet through the IPv6 address. After you create a FlexusX instance, you need to enable IPv6 so that the instance dynamically obtains an IPv6 address. For details, see **Dynamically Assigning IPv6 Addresses**. **NOTE** • IPv6 can only be enabled during instance creation. Once enabled, this setting cannot be modified. If **IPv6 Bandwidth** is not enabled during instance creation, you can enable it after the instance is created. • Dedicated bandwidth is not supported.

Parameter	Description
Security Group	You can select an existing security group from the drop-down list or create a new one. This configuration controls access to FlexusX instances within a security group or among security groups, enhancing instance security. You can define access rules for a security group to protect the FlexusX instances in the group. When creating a FlexusX instance, you can select multiple security groups (no more than five is recommended). The access rules of all the selected security groups apply to the instance. The security group rules affect the access and use of FlexusX instances. For details about how to configure a security group rule, see **Configuring Security Group Rules for a FlexusX Instance**. Enable the following common protocols and ports as needed: • Port 80: default port for web page access through HTTP. • Port 443: port for web page access through HTTPS. • ICMP: used to ping FlexusX instances to check their communication statuses. • Port 22: reserved for logging in to Linux FlexusX instances using SSH. • Port 3389: reserved for remote desktop login to Windows FlexusX instances.

EIP

An EIP is a static public IP address bound to a FlexusX instance in a VPC. The EIP enables the instance to communicate with the Internet.

Figure 2-7 EIP parameters

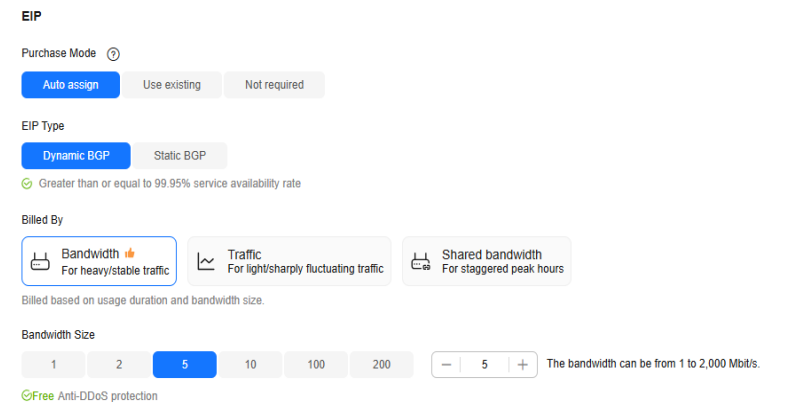


Table 2-6 EIP parameters

Parameter	Description
Purchase Mode	• **Auto assign**: The system automatically assigns an EIP with a dedicated bandwidth to each FlexusX instance. The bandwidth is configurable. • **Using existing**: An existing EIP will be assigned to the FlexusX instance. If you select an existing EIP, batch creation of FlexusX instances is disabled. • **Not required**: A FlexusX instance without an EIP cannot access the Internet. However, it can still be used as a FlexusX instance or be deployed in a cluster on a private network.
EIP Type	This parameter is mandatory when **Purchase Mode** is set to **Auto assign**. • **Dynamic BGP**: If there are changes on a network using dynamic BGP, network configurations can be promptly adjusted using the specified routing protocol, ensuring network stability and optimal user experience. • **Static BGP** If there are changes on a network using static BGP, network configurations cannot be promptly adjusted and user experience may be affected.
Billed By	This parameter is mandatory when **Purchase Mode** is set to **Auto assign**. If you select **Bandwidth** or **Traffic**, the system will allocate a dedicated bandwidth for you, and the bandwidth is dedicated for one EIP. • **Bandwidth**: You will be billed based on the amount of bandwidth you configure. • **Traffic**: You will be billed based on the actual traffic you have used. • **Shared bandwidth**: You will be billed by the bandwidth shared by multiple EIPs.
Bandwidth Size	Select the bandwidth size (in Mbit/s) based on service requirements.

(Optional) Associated Services

Configure Cloud Eye and Host Security Service (HSS) based on your **needs**.

Figure 2-8 Associated services

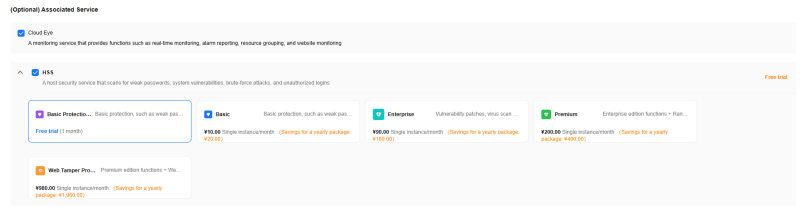


Table 2-7 Associated services

Parameter	Description
Cloud Eye	If you enable Cloud Eye, an agent will be automatically installed on your FlexusX instance to provide 1-minute fine-grained monitoring of its metrics, such as vCPUs, memory, network, disks, and processes.
HSS	If you enable HSS, your FlexusX instance will be provided with host security services that scan for weak passwords, system vulnerabilities, brute-force attacks, and unauthorized logins. You can select the HSS edition as required. The basic protection trial edition is free for one month. After one month, HSS stops providing services.

FlexusX Instance

Figure 2-9 Configuring the FlexusX Instance

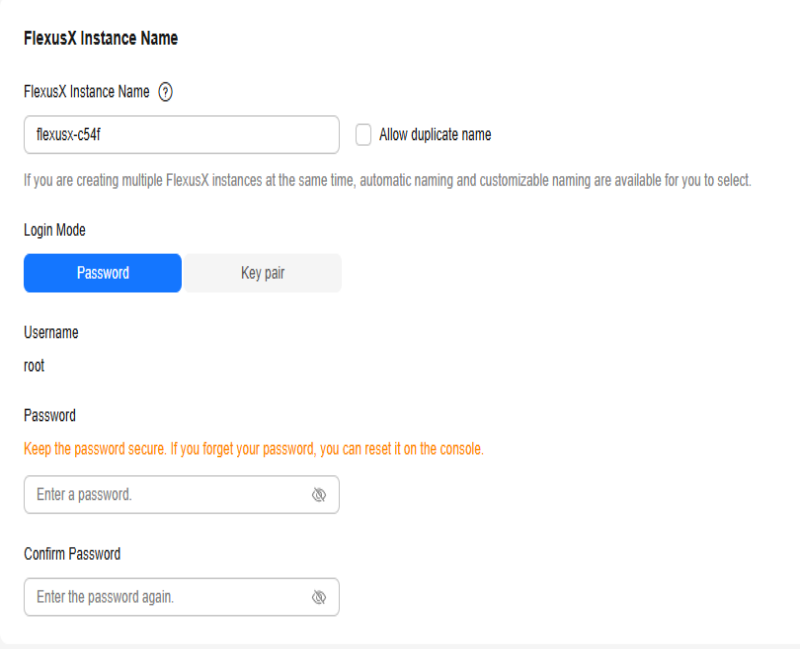


Table 2-8 Parameters required for configuring the FlexusX Instance

Parameter	Description
FlexusX Instance Name	You can create a custom FlexusX instance name. If you purchase multiple FlexusX instances at a time, the system automatically sequences these instances.

Parameter	Description
Login Mode	• **Password**: A username and its initial password are used for FlexusX instance login authentication. • **Key pair**: A key pair is used for FlexusX instance login authentication. You can select an existing key pair, or click **Create Key Pair** to create a new one. **NOTE** If you choose to use an existing key pair, ensure that it is available locally, or you will not be able to log in to your FlexusX instance. • **Password from image**: If a password has been set for the private image, you can select this option to use that password. • **Set password later**: You can choose to set a password for your FlexusX instance later. If you select this option, remember to set a password after your FlexusX instance is created.

Cloud Backup and Recovery

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

Figure 2-10 Configuring CBR parameters

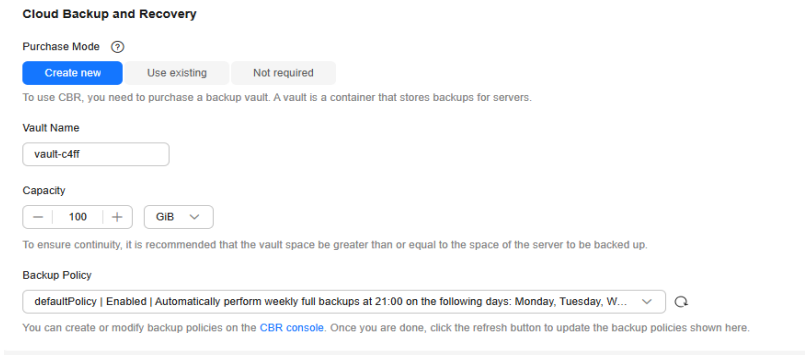


Table 2-9 CBR parameters

Parameter	Description
Create new	• **Vault Name**: The vault name cannot exceed 64 characters. Only letters, digits, underscores (_), and hyphens (-) are supported. for example, **vault-f61e**. The default naming rule is **vault**_*xxxx*. • Capacity: Enter the vault capacity, which is required for backing up the FlexusX instance. The vault capacity cannot be smaller than that of the FlexusX instance to be backed up. Its value ranges from the total capacity of the FlexusX instance to 10,485,760 in the unit of GB. • **Backup Policy**: Select a backup policy from the drop-down list, or go to the CBR console and configure a desired one.
Use existing	• **Vault**: Select an existing vault from the drop-down list. • **Backup Policy**: Select a backup policy from the drop-down list, or go to the CBR console and configure a desired one.
Not required	Backup is not configured. If you require this function after purchasing the FlexusX instance, log in to the CBR console and bind the desired cloud backup vault to your FlexusX instance.

(Optional) Advanced Options

Figure 2-11 Advanced settings

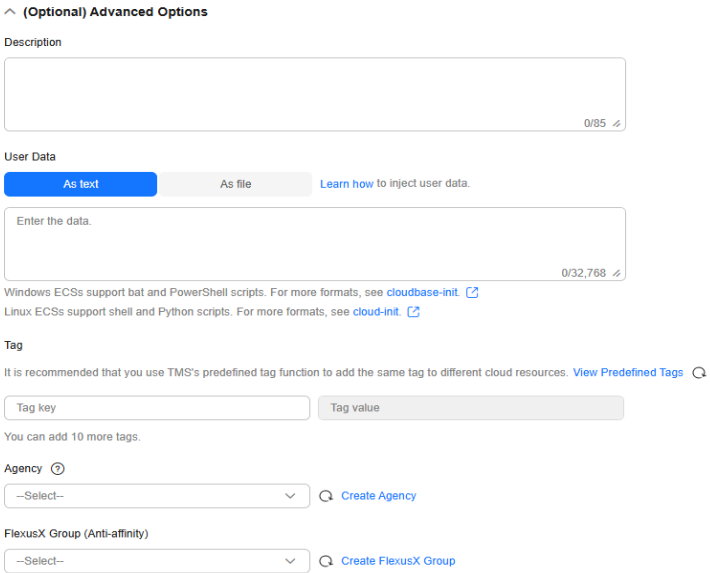


Table 2-10 Advanced settings

Parameter	Description
Description	Add a FlexusX instance description.
User Data	This parameter is available only if you select **Key pair** for **Login Mode**. You can inject user data to customize your FlexusX instance. With this configuration, the FlexusX instance automatically injects data the first time it starts up. • **As text**: allows you to enter the user data in the text box. • **As file**: allows you to inject script files or other files when you create a FlexusX instance. For example, if you activate user **root** with a script, you can log in to the FlexusX instance as **root**. For details about how to pass user data, see **Passing User Data to ECSs**.
Tag	Tags the FlexusX instance. Adding tags to FlexusX instances helps you better identify and manage your FlexusX instances. You can add up to 10 tags to each instance. **NOTE** Tags added during the instance creation will also be added to the EIP and EVS disks (including the system disk and data disks) of the FlexusX instance. If the instance uses an existing EIP, the tags will not be added to that EIP. After creating the instance, you can view the tags on the pages providing details about the FlexusX instance, EIP, and EVS disks.
Agency	When your FlexusX resources need to be shared with other accounts, or your FlexusX is delegated to professional personnel or team for management, the tenant administrator creates an agency in IAM and grants the FlexusX management permissions to the personnel or team. The delegated account can log in to the cloud system and switch to your account to manage resources. This way, you do not need to share security credentials (such as passwords) with other accounts, ensuring the security of your account. If you have created an agency in IAM, select the agency from the drop-down list. For more information about agencies, see **Account Delegation**.
FlexusX Group (Anti-affinity)	Select the FlexusX instance group you want to add your FlexusX instance to. A FlexusX instance group applies the anti-affinity policy to the instances in it so that they can be distributed on different hosts. For details about how to create a FlexusX instance group, see **Managing a FlexusX Instance Group**.

Step 3: Confirm the Configuration and Submit the Order

1. Click **Next: Confirm**.

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

   Table 2-11 Verifying parameter configuration

Parameter	Description
Enterprise Project	This function is provided for enterprise users. An enterprise project makes it easy to manage projects and groups of cloud resources and users. Use the default enterprise project or create one. Select an enterprise project from the drop-down list. For more details, see **Accessing the Enterprise Center**.
Required Duration	Specifies the subscription duration of the FlexusX instance. This parameter is displayed only when **Billing Mode** is set to **Yearly/Monthly**.
Auto-renew	This parameter is displayed only when **Billing Mode** is set to **Yearly/Monthly**. You can select **Auto-renew** to automatically renew a yearly/monthly subscription upon expiry. • Monthly subscription: auto-renews for 1 month every time. • Yearly subscription: auto-renews for 1 year every time. For more information about auto-renewal rules, see **Auto-Renewal Rules**.
Required Duration	This parameter is displayed only when **Billing Mode** is set to **Pay-per-use**. You can select **Set scheduled deletion time** and set the time for deleting the FlexusX instance. This way, the FlexusX instance will be deleted automatically as scheduled. However, before the scheduled time arrives, you can change it on the instance details page. **NOTE** Back up data before you set the scheduled deletion time.
Quantity	You can set how many FlexusX instances to be created in a batch. FlexusX instances created in a batch have the same configurations.

2. Read and agree to the agreement/disclaimer.
3. Hover your mouse over the price to learn about price details.
4. Click **Submit** and complete the payment.
5. Go back to the FlexusX console and view the purchased FlexusX instances.

Helpful Links

- If you did not create a password for your FlexusX instance or if you have forgotten the login password, **reset the password** and then log in to the instance.
- After creating a FlexusX instance, you can remotely connect to the instance to deploy it. For details, see **Logging In to a FlexusX Instance**.

  Before logging in to a FlexusX instance in non-VNC mode, ensure that the login port has been allowed by security group rules. Otherwise, the login fails. To log in to a Linux instance, ensure that SSH port 22 has been allowed. To log in to a Windows instance, ensure that RDP port 3389 has been allowed. For details about how to configure security group rules, see **Configuring Security Group Rules for a FlexusX Instance**.
- Data disks can be used only after **initialization**.
- If you want to deploy your FlexusX instance by yourself, refer to the instructions in **Setting Up Websites**.

  NOTE

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

3 Logging In to a FlexusX Instance

3.1 Login Modes

You can log in to a FlexusX instance using different login methods depending on the instance OS.

Windows FlexusX Instance Login Overview

The FlexusX instance login mode depends on the local OS. You can select the login mode best suited to your local OS.

Table 3-1 Windows FlexusX instance login modes

Instance OS	Local OS	Login Mode	Requirements
Windows	Windows	Use MSTSC. The method is the same as logging in to an ECS. **Logging In to a Windows ECS from a Windows Server**	The FlexusX instance must have an EIP bound. (If you log in to a FlexusX instance through an intranet, for example, through VPN or Direct Connect, the instance does not require an EIP.)
	Linux	Install a remote connection tool, such as rdesktop. The method is the same as logging in to an ECS. **Logging In to a Windows ECS from a Linux Server**	
	macOS	Install a remote connection tool, such as Microsoft Remote Desktop for Mac. The method is the same as logging in to an ECS. **Logging In to a Windows ECS from a macOS Server**	

Instance OS	Local OS	Login Mode	Requirements
	Mobile terminal	Install a remote connection tool, such as Microsoft Remote Desktop. The method is the same as logging in to an ECS. **Logging In to a Windows ECS from a Mobile Terminal**	
	Windows	Use the management console. For details, see **Logging In to a FlexusX Instance Using VNC**.	No EIPs are required.

Linux FlexusX Instance Login Overview

The FlexusX instance login mode depends on the local OS. You can select the login mode best suited to your local OS.

Table 3-2 Linux FlexusX instance login modes

Instance OS	Local OS	Login Mode	Requirements
Linux	Windows	(Recommended) Use CloudShell provided on the management console to log in to a FlexusX instance. **Logging In to a Linux FlexusX Instance Using CloudShell** **NOTE** Currently, CloudShell is only available in some regions. For details, see the management console.	The FlexusX instance must have an EIP bound. (If you log in to a FlexusX instance through an intranet, for example, through VPN or Direct Connect, the instance does not require an EIP.)
	Windows	Use remote login tools, such as PuTTY and Xshell, to log in to a FlexusX instance. The method is the same as logging in to an ECS. • Using an SSH password: **Logging In to a Linux ECS from a Local Windows Server** • Using an SSH key pair: **Logging In to a Linux ECS from a Local Windows Server**	

Instance OS	Local OS	Login Mode	Requirements
	Linux	Use commands to log in to a FlexusX instance. The method is the same as logging in to an ECS. • Using an SSH password: **Logging In to a Linux ECS from a Local Linux Server** • Using an SSH key pair: **Logging In to a Linux ECS from a Local Linux Server**	
	Mobile terminal	Use SSH client tools, such as Termius and JuiceSSH, to log in to a FlexusX instance. The method is the same as logging in to an ECS. **Logging In to a Linux ECS from a Mobile Terminal**	
	macOS	Use the macOS terminal to log in to a FlexusX instance. The method is the same as logging in to an ECS. **Logging In to a Linux ECS from a macOS Server**	
	Windows	Use the management console. For details, see **Logging In to a FlexusX Instance Using VNC**.	No EIPs are required.

NOTE

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

Helpful Links

- **Multi-User Login Issues**
- **Why Can't I Log In to My Windows ECS?**
- **What Are the Username and Password for Remotely Logging In to a FlexusX Instance?**
- **What Can I Do If I Forget the Login Password of a FlexusX Instance?**

3.2 Logging In to a FlexusX Instance Using VNC

Scenarios

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

If you cannot use the MSTSC or other remote login tools to log in to a FlexusX instance, 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.

Prerequisites

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

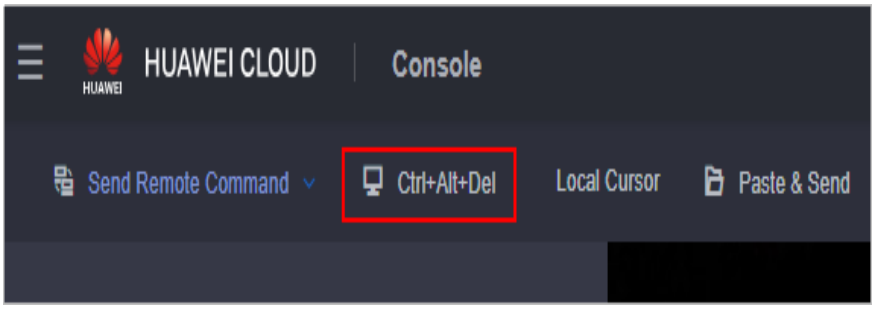
Procedure

1. Log in to the FlexusX **console**. In the upper left corner, click  and select a region.
2. Locate the FlexusX instance you want to log in to, click **Remote Login** in the **Operation** column.
3. Log in to the FlexusX instance as prompted.

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

   - For 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 as prompted.

     The default username is **root**.

Helpful Links

- **Multi-User Login Issues**
- **Why Can't I Log In to My Windows ECS?**
- **What Are the Username and Password for Remotely Logging In to a FlexusX Instance?**
- **What Can I Do If I Forget the Login Password of a FlexusX Instance?**

3.3 Logging In to a Linux FlexusX 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 cloud servers through the CloudShell proxy IP address. This helps hide your real IP address to improve your privacy and cloud server security.

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

NOTE

Currently, CloudShell is only available in some regions. For details, see the management console.

Prerequisites

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

  The username created from a public image is **root**.
- Ensure that the remote port (default SSH port: 22) of the CloudShell proxy IP address is allowed in the security group. Otherwise, the FlexusX instance 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 FlexusX Instance**.

If a different port is required, you can use the default port to log in to the FlexusX instance and then change the port No. For details about how to change a remote login port, see **How Can I Change a Remote Login Port?**

- An EIP has been bound to the FlexusX instance.
- You can use CloudShell to connect to a FlexusX instance 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 FlexusX **console**. In the upper left corner, click and select a region.
2. Locate the FlexusX instance you want to log in to, click **Remote Login** in the **Operation** column.
3. In the displayed dialog box, click **Log In** in **CloudShell Login**.
4. On the CloudShell page, configure the FlexusX instance information.

   Upon the first login, the CloudShell wizard is displayed by default. You need to enter the instance information for connection.

NOTE

You can use the EIP or private IP address to log in to the FlexusX instance.

- If you select the EIP bound to the FlexusX instance:
  i. Configure parameters for logging in to the FlexusX instance.

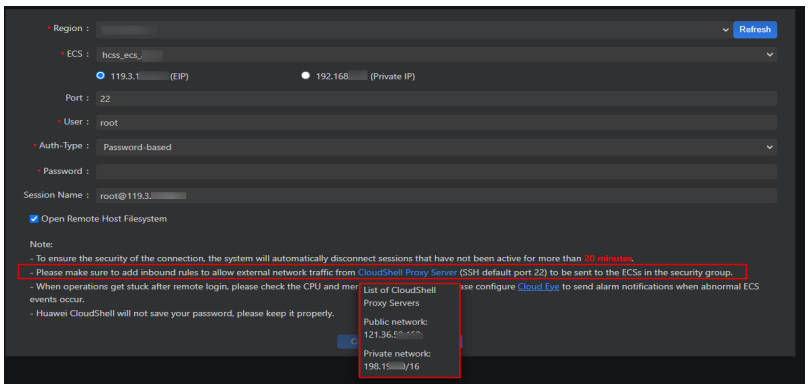
Table 3-3 Parameters for logging in to the FlexusX instance

Parameter	Description
Port	The port for connecting to the FlexusX instance. The default value is 22.
User	The username of the FlexusX instance. The default value is **root**.
Auth-Type	Select **Password-based** and enter the password for logging in to the FlexusX instance. If you did not set the password or forgot the password, reset it by referring to **Resetting the Password for a FlexusX Instance**.
Session Name	The default format is *Username@IP address*. You can change it as needed.

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

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

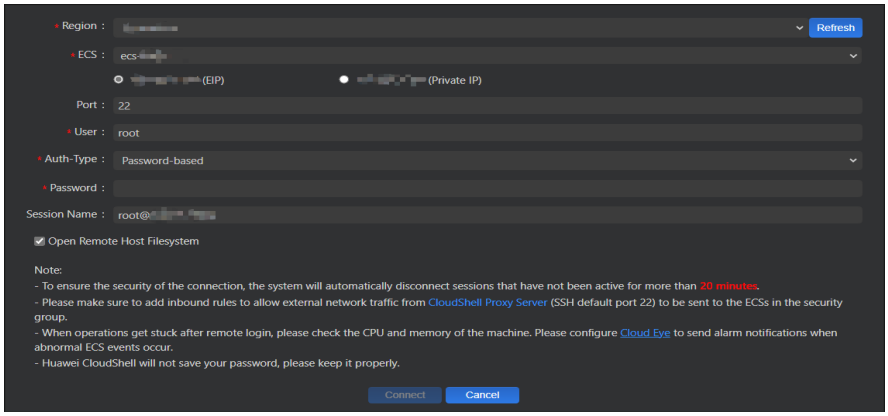
Figure 3-2 CloudShell proxy IP address



ii. Click **Connect** to log in to the instance.

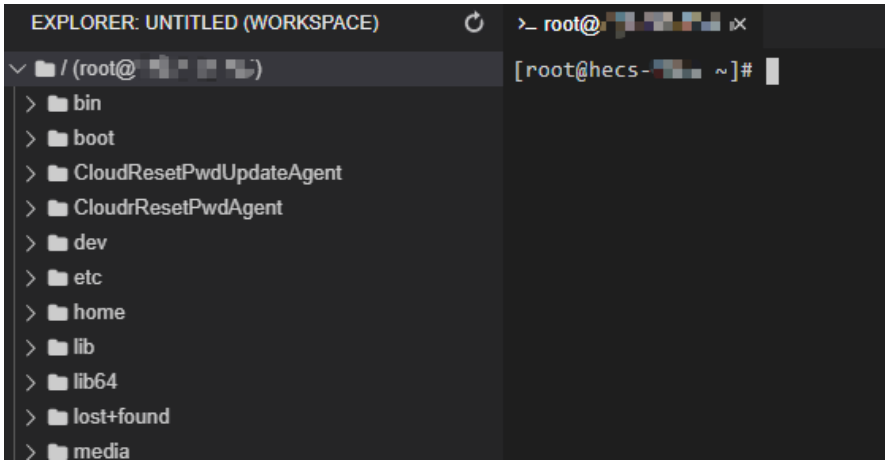
If the system does not respond, the login password is incorrect or the password has not been set. In this case, reset the password and log in to the instance again.

Figure 3-3 CloudShell wizard (EIP)



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

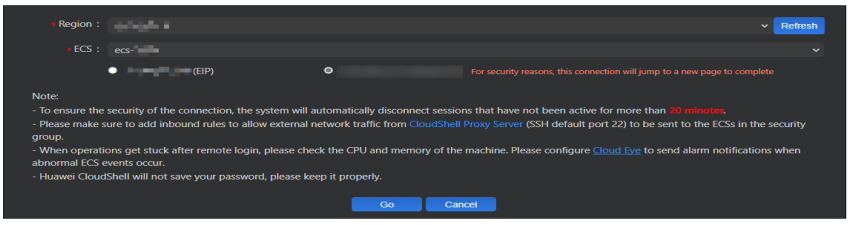
Figure 3-4 Successful login



– If you select the private IP address of the FlexusX instance:

i. Click **Go**.

Figure 3-5 Going to the CloudShell wizard (private IP address)



> **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 **prerequisites** first.

ii. Configure parameters for logging in to the FlexusX instance.

Figure 3-6 CloudShell wizard (private IP address)

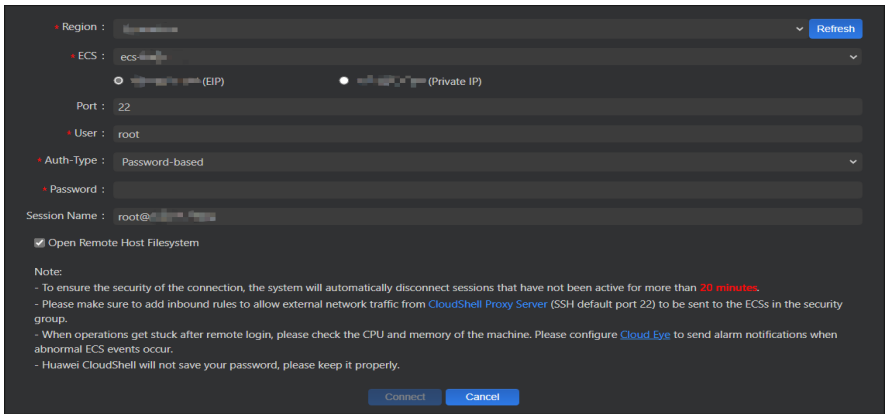


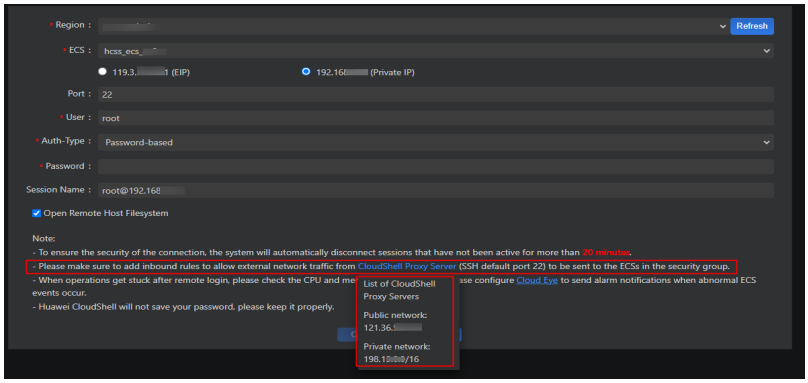
Table 3-4 Parameters for logging in to the FlexusX instance

Parameter	Description
Port	The port for connecting to the FlexusX instance. The default value is 22.
User	The username of the FlexusX instance. The default value is **root**.
Auth-Type	Select **Password-based** and enter the password for logging in to the FlexusX instance. If you did not set the password or forgot the password, reset it by referring to **Resetting the Password for a FlexusX Instance**.
Session Name	The default format is *Username@IP address*. You can change it as needed.

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

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

Figure 3-7 CloudShell proxy IP address

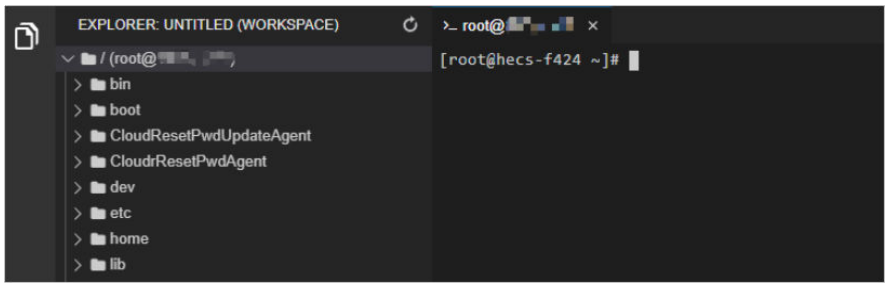


iii. Click **Connect** to log in to the instance.

If the system does not respond, the login password is incorrect or the password has not been set. In this case, reset the password and log in to the instance again.

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

Figure 3-8 Successful login



Helpful Links

- After login, if you need to use the copy-and-paste function provided by CloudShell, see **Common CloudShell Operations**.
- **Why Can't I Log In to My Linux ECS?**
- **What Are the Username and Password for Remotely Logging In to a FlexusX Instance?**
- **What Can I Do If I Forget the Login Password of a FlexusX Instance?**

4 Managing FlexusX Instances

4.1 Resetting the Password for a FlexusX Instance

Scenarios

If you select **Password** as the login credential when purchasing a FlexusX instance, you can log in to the FlexusX instance using the username and password. Keep your password secure.

If you did not set a password when creating a FlexusX instance, if you have forgotten the password, or if the password has expired, you can reset the password on the management console.

Constraints

You can only reset the password if the FlexusX instance is in the **Stopped** or **Running** state. If you reset the password when the FlexusX instance is in **Running** state, the password change will not be applied until the instance is restarted.

Prerequisites

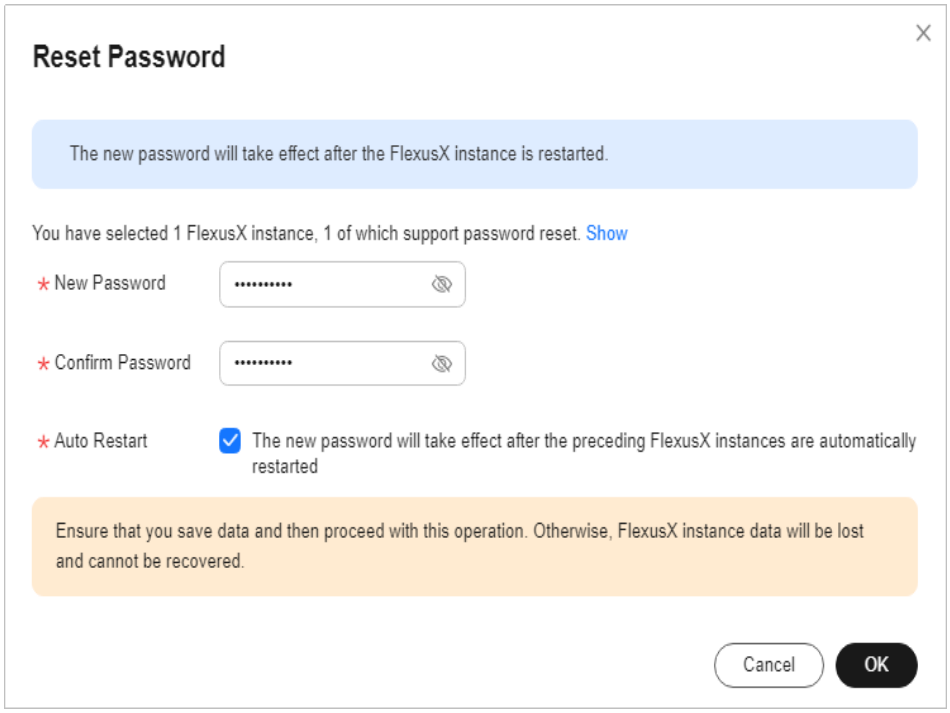
- The one-click password reset plug-in must have been installed.
  - If your FlexusX instance was created using a public image, the password reset plug-in was installed on the instance by default.
  - If your FlexusX instance was created using a private image and has no password reset plug-in installed,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

Procedure

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

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

   Figure 4-1 Reset Password



3. Set and confirm a new password as prompted.

   If you reset the password for a running FlexusX instance, the password change is not applied until the next restart. Select **Auto Restart**.

   The new password must meet the password complexity requirements.

Table 4-1 Parameters for resetting the password online

Parameter	Description
New Password	Specifies 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 !@%-_=+[]:./^,{}? (only applied to Linux) !@%-_=+[]:./? (only applied to Windows) • Cannot contain the username or the username spelled backwards. • Cannot contain more than two consecutive characters in the username (applying only to Windows FlexusX instances). • Cannot start with a slash (/) (applying only to Windows FlexusX instances).
Confirm Password	Must be the same as the new password.

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

Helpful Links

- **Logging In to a FlexusX Instance Using VNC**
- **What Are the Username and Password for Remotely Logging In to a FlexusX Instance?**

4.2 Changing the OS of a FlexusX Instance

4.2.1 Reinstalling the OS of a FlexusX Instance

Scenarios

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

Prerequisites

The target FlexusX instance has a system disk attached.

Notes

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

Billing

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

Procedure

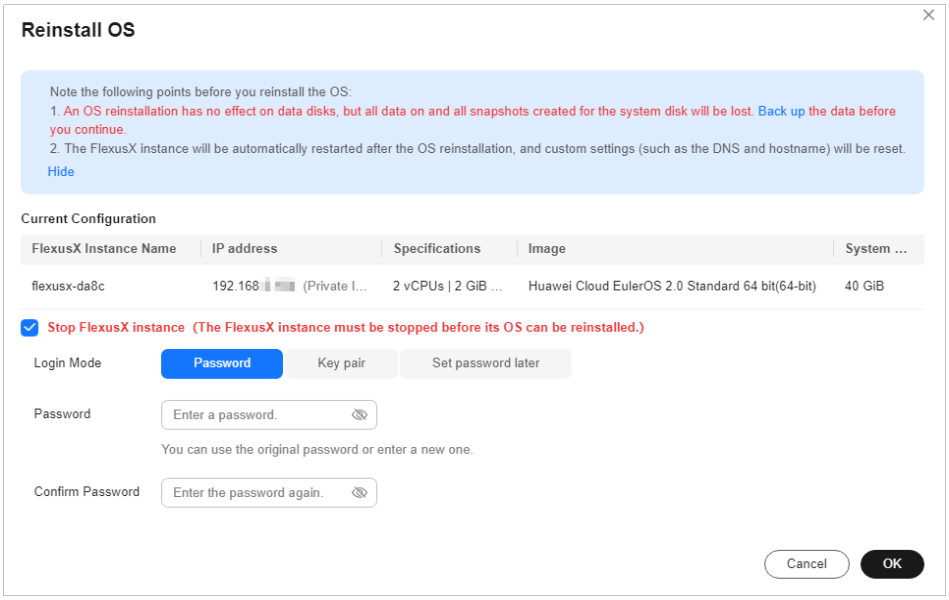
1. Log in to the FlexusX **console**. In the upper left corner, click and select a region.
2. Locate the FlexusX instance and choose **More** > **Manage Image** > **Reinstall OS** in the **Operation** column.
3. Specify the parameters required for reinstalling the OS.
   - Select **Stop FlexusX instance**. The FlexusX instance must be stopped before its OS can be reinstalled.
   - Set **Login Mode**. The credentials are used for logging in to the FlexusX instance.
     - **Password**: A username and its initial password are used for FlexusX instance login authentication.

       The initial password of user **root** is used for login authentication in Linux, and the initial password of user **Administrator** is used for login authentication in Windows.
     - **Key pair**: A key pair is used for FlexusX instance login authentication. You can select an existing key pair, or click **Create Key Pair** to create a new one.

NOTE

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

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



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

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

Follow-Up Operations

If the OS reinstallation fails, try again. If the second attempt still fails, **submit a service ticket**.

4.2.2 Changing the OS of a FlexusX Instance

Scenarios

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

NOTICE

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

Notes

- An OS change does not change any FlexusX instance specifications.
- After the OS is changed, the IP address of the FlexusX instance remains unchanged.
- After the OS is changed, the original OS will be gone. All the data in all the partitions of the system disk (including the system partition) will be lost, so back up the system disk data before the change.
- Changing the OS will not affect data on data disks.
- After the OS is changed, your service environment must be deployed in the new OS again.
- After the OS is changed, the FlexusX instance will automatically restart.
- Do not perform any operations on the FlexusX instance immediately after its OS is changed. Wait for several minutes while the system injects the password or key. Otherwise, the injection may fail, and the FlexusX instance cannot be logged in to.

Constraints

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

Billing

The new system disk may have a larger capacity after an OS change, so the pricing may increase. For details, see **Product Pricing Details**.

Procedure

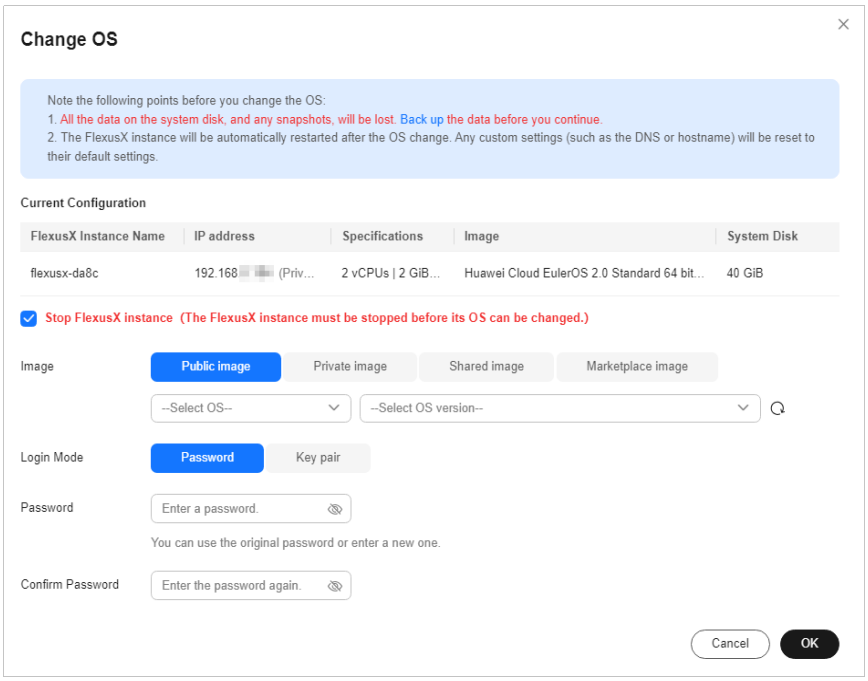
1. Log in to the FlexusX **console**. In the upper left corner, click  and select a region.
2. Locate the FlexusX instance and choose **More** > **Manage Image** > **Change OS** in the **Operation** column.
3. Specify the parameters required for changing the OS.
   - Select **Stop FlexusX instance**.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

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

NOTE

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

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



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

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

Follow-Up Operations

If the OS change fails, try again. If the second attempt still fails, **submit a service ticket**.

4.3 Modifying the Specifications of a FlexusX Instance

Scenarios

If the FlexusX instance you purchased cannot meet service requirements, you can upgrade the vCPUs and memory by modifying the instance specifications or change the instance to an ECS.

Notes

- Downgrading FlexusX instance specifications (vCPUs or memory) will reduce performance.
- The specifications of a FlexusX instance cannot be modified when the instance is in an intermediate state, such as starting, stopping, resetting the OS, or migrating, or when the capacity of EVS disks used by the instance is being expanded.
- Before modifying the specifications of a Windows instance, modify the SAN policy by following the instructions provided in **What Should I Do If a Disk Is Offline?** in the ECS documentation to prevent offline disks after the specifications are modified.
- A specification change failure may result in data loss for the FlexusX instance. Back up the data before the change. For details, see **Backing Up a FlexusX Instance**.

Constraints

The selected instances must use the same billing mode, use the same flavor, and be in the same AZ.

Billing

Modifying specifications will change how much you are billed for the instances. For details, see **Pricing of a Changed Specification**.

Preparations

If the NIC retaining is enabled in the OS, NIC flapping may happen after the instance specifications are modified. To prevent such issues, perform the following operations before modifying the specifications:

- Linux

  Run the following commands on the ECS to delete the files with both **persistent** and **net** included in their names from the network rule directory:

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

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

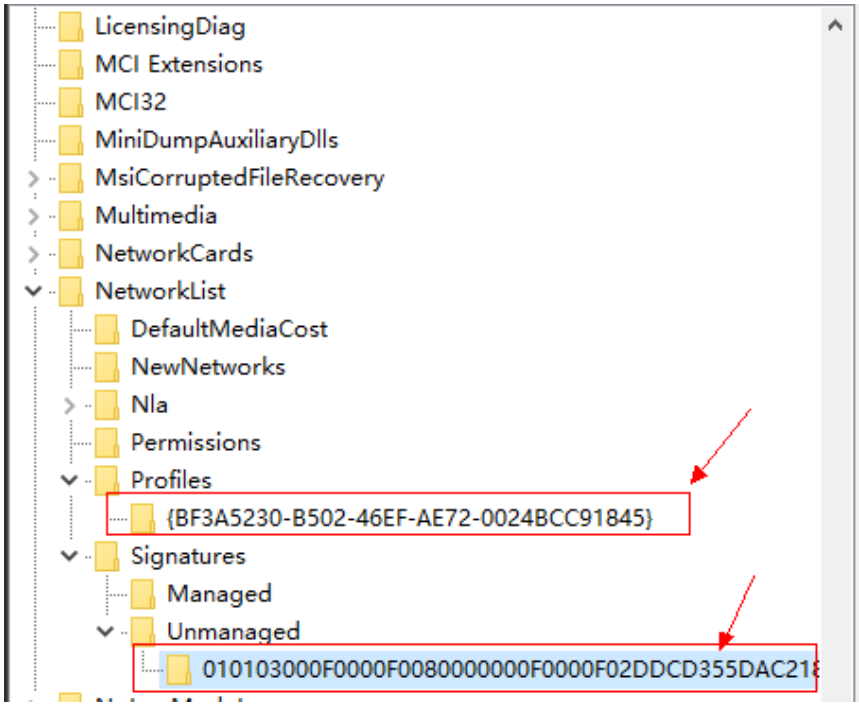
- Windows

  Delete the following directories from the registry on the ECS:

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged

Figure 4-2 Registry



For more information about network interface flapping, see **What Should I Do If NIC Flapping Occurs After My ECS Specifications Are Modified?**

Procedure

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

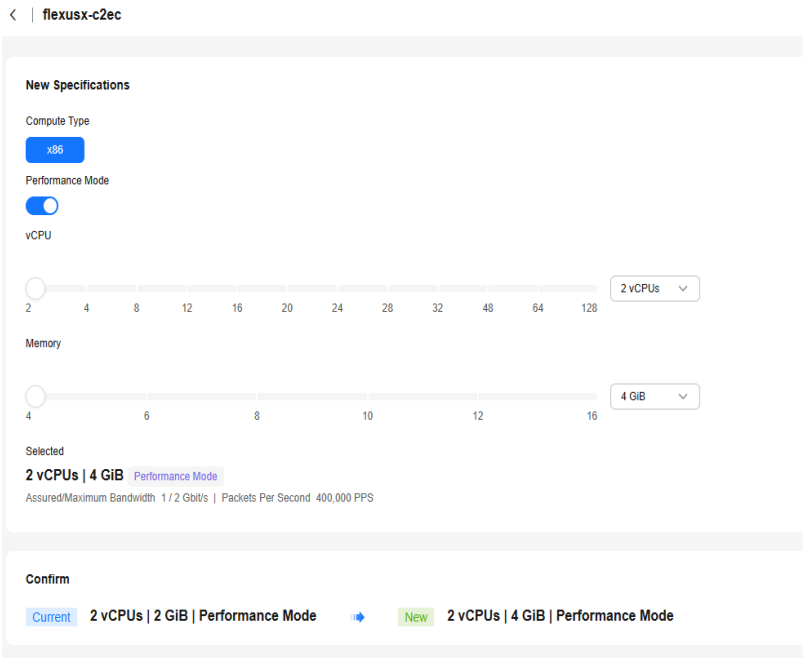
Modifying the Specifications of a FlexusX Instance

1. Log in to the FlexusX **console**. In the upper left corner, click and select a region.
2. Locate the FlexusX instance and choose **More** > **Modify Specifications** in the **Operation** column.
3. On the displayed page, select desired instance specifications.

   FlexusX has a performance mode option to provide fantastic, stable performance at additional charges. For more information, see **Enabling Performance Mode for a FlexusX Instance**.

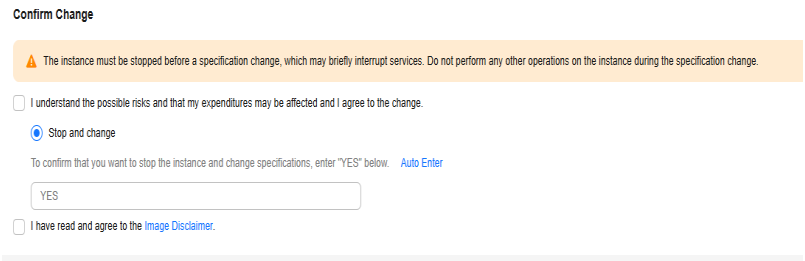
   - Select new specifications.

Figure 4-3 New specifications



– Confirm the change.

Figure 4-4 Confirming the change

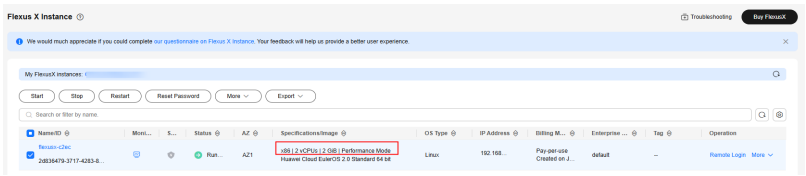


- If you select **Stop and change**, the specifications are modified after automatic system shutdown.
- If **Apply for Live Change** is selected, the specifications can be modified without system shutdown. The live change function is in the open beta testing (OBT) phase. Apply for the function as needed. If this option is not displayed on the console, live change is not supported. For details about live change, see **What Is Live Change?**

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

   After the modification is complete, check whether the new specifications are displayed on the FlexusX instance list page.

Figure 4-5 Viewing new specifications

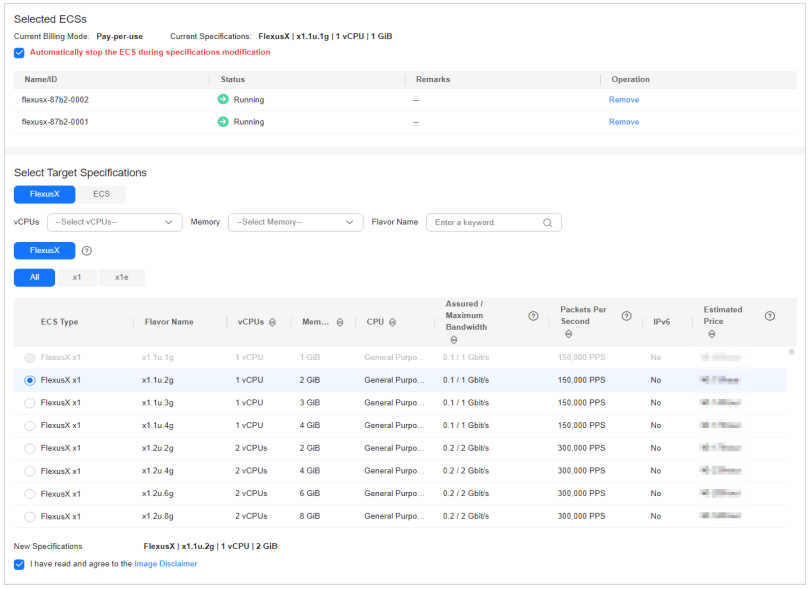


Batch Modifying Specifications of FlexusX Instances

1. Log in to the FlexusX **console**. In the upper left corner, click and select a region.
2. Select the FlexusX instances whose specifications you want to modify, choose **More** > **Modify Specifications** above the list, and click **For Pay-per-Use FlexusX Instances** or **For Yearly/Monthly FlexusX Instances**.
3. On the displayed page, select desired instance specifications.
   - Before modifying the specifications, stop the cloud server or select **Automatically stop the ECS during specifications modification**.
   - Select new specifications.

     FlexusX X1 instances have performance mode disabled, and FlexusX X1e instances have performance mode enabled.

Figure 4-6 Batch modifying specifications



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

   After the change, if you selected FlexusX specifications, check whether the new specifications are displayed on the FlexusX instance list page. If you selected ECS specifications, check whether the new specifications are displayed on the ECS list page.

Figure 4-7 Viewing new specifications

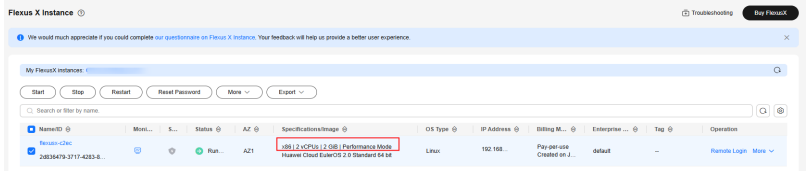
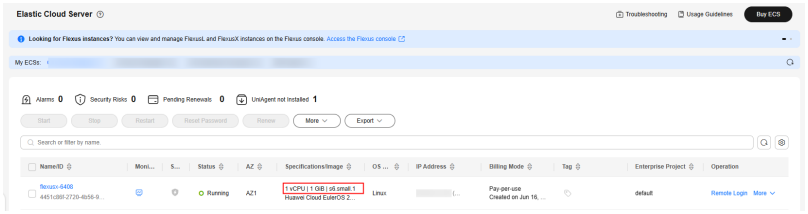
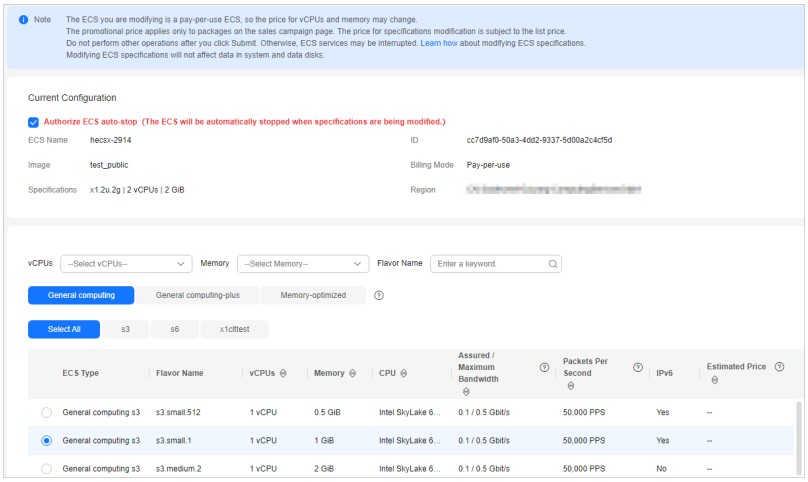


Figure 4-8 Viewing new specifications on the ECS list page



Changing a FlexusX Instance to an ECS

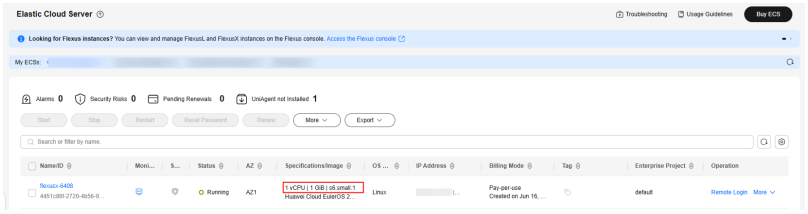
1. Log in to the FlexusX **console**. In the upper left corner, click and select a region.
2. Locate the row that contains the target FlexusX instance and choose **More** > **Change to ECS** in the **Operation** column.
3. On the displayed page, select desired instance specifications.
   - Before modifying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



4. Click **Next**.
5. Confirm the settings, read and select the disclaimer, and then click **Submit**.

   Wait until the modification is complete and check whether the new specifications are displayed on the ECS list page.

Figure 4-9 Viewing new specifications on the ECS list page



Follow-Up Operations

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

- Linux: For details, see **Why Does Disks Fail to Be Mounted After I Modify the Specifications of a Linux ECS?**

Helpful Links

- **Do I Need to Stop My FlexusX Instance If I Want to Enable or Disable Performance Mode for It?**
- **Can I Enable Performance Mode After a FlexusX Instance Is Created?**
- **How Do I Use Live Change?**

4.4 Enabling Performance Mode for a FlexusX Instance

Scenarios

FlexusX provides flexible compute resources with QoS-guaranteed performance. FlexusX instances perform as well as exclusive instances most of the time but may occasionally underperform. To meet the strict performance requirements of certain workloads, such as rendering and HPC applications, FlexusX has a performance mode option. If this option is enabled, your FlexusX instances are bound with the underlying CPU cores, so they can provide stable, fantastic QoS-guaranteed performance.

Table 4-2 lists the differences between FlexusX instances where the performance mode is enabled and disabled. For details about the differences between FlexusX instance specifications, see **Instance Specifications**.

Table 4-2 Differences between FlexusX instances where the performance mode is enabled and disabled

Performance Mode	Enabled	Disabled
Scenarios	Web 3.0 application development, rendering, cryptocurrency, ERP, game servers, e-commerce livestreaming, e-commerce going global, enterprise website building, applet development, and development and testing	E-commerce going global, enterprise website building, applet development, development and testing, enterprise resource planning (ERP), game servers, and e-commerce livestreaming
vCPU allocation logic	CPU cores bound to provide QoS-guaranteed fantastic, stable performance	Flexible compute with QoS-guaranteed performance, close to exclusive instances

Performance Mode	Enabled	Disabled
Compute resources	• vCPU/Memory ratio: flexible custom ratios to meet your specific needs with low-cost resources • vCPU/Memory range: 2 to 32 vCPUs and 2 to 256 GiB of memory • Basic/Turbo frequency: 2.45 GHz/3.5 GHz and 2.4 GHz/3.7 GHz	• vCPU/Memory ratio: flexible custom ratios to meet your specific needs with low-cost resources • vCPU/Memory range: 1 to 16 vCPUs and 1 GiB to 128 GiB of memory • Processor: 3rd Generation Intel® Xeon® Scalable Processor • Basic/Turbo frequency: 2.8 GHz/3.5 GHz and 2.6 GHz/3.4 GHz

Precautions

During this process, you may also need to modify the instance specifications if there are insufficient underlying resources.

Billing

Additional charges are required for the performance mode.

Enabling Performance Mode

You can enable performance mode for a FlexusX instance during or after the instance creation.

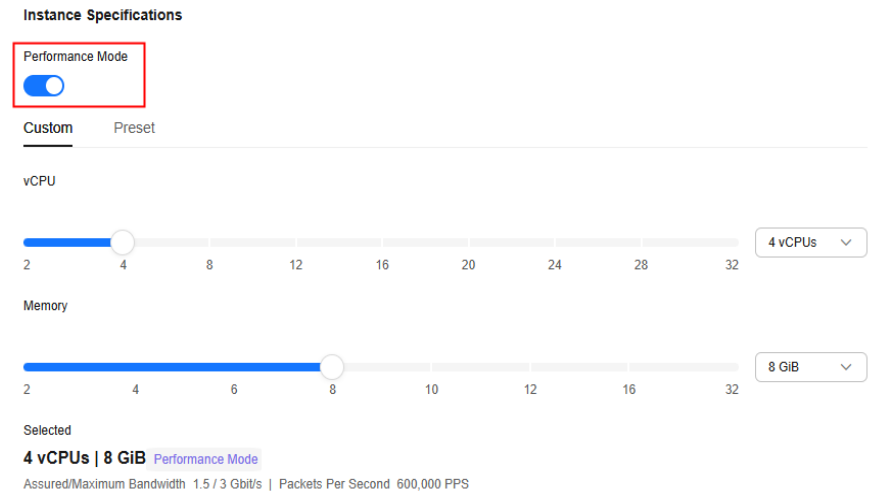
NOTE

Performance mode is only available in some regions. For details, see the information displayed on the management console.

- **Enabling performance mode when purchasing a FlexusX instance**

  Once the instance is created, you can enjoy stable, ample performance immediately.

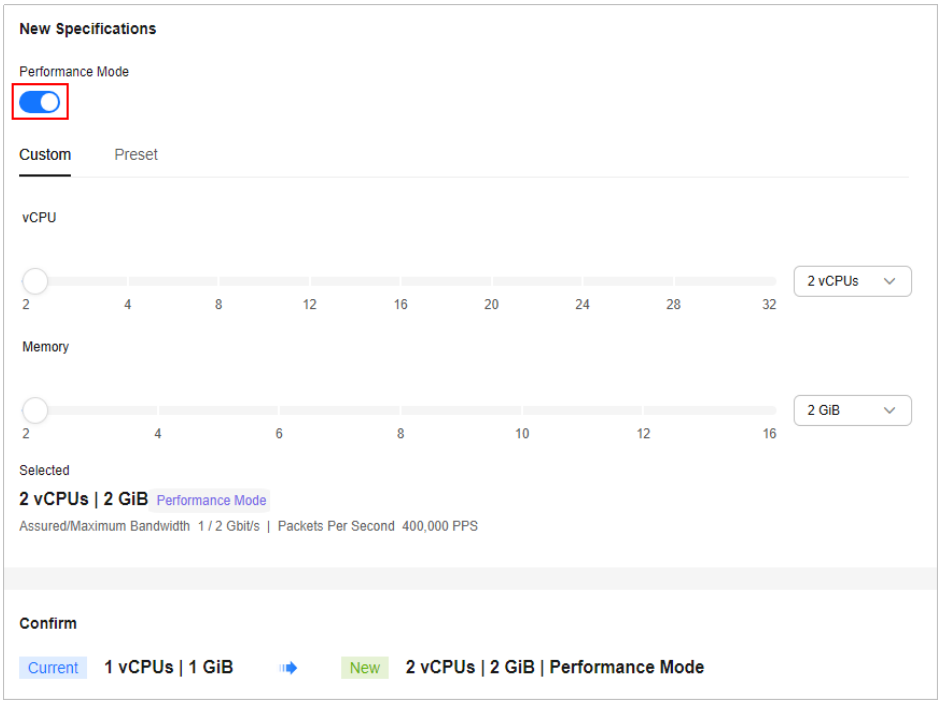
Figure 4-10 Enabling performance mode during purchase



- **Enabling performance mode after a FlexusX instance is purchased**

  You can enable performance mode for the instance using the **Modify Specifications** option. During this process, you may also need to modify the instance specifications if there are insufficient underlying resources. For details about how to modify specifications, see **Modifying the Specifications of a FlexusX Instance**.

  Figure 4-11 Enabling performance mode using the **Modify Specifications** option



FAQs

You may encounter the following issues when using performance mode:

- **How Do I Know Whether Performance Mode Is Enabled for a FlexusX Instance?**
- **How Much Can Performance Be Improved If Performance Mode Is Enabled for a Flexus X Instance?**
- **Do I Need to Stop My FlexusX Instance If I Want to Enable or Disable Performance Mode for It?**
- **Can I Enable Performance Mode After a FlexusX Instance Is Created?**
- **Will I Continue to Be Billed If I Disable Performance Mode for My FlexusX Instance?**

4.5 Managing a FlexusX Instance Group

Scenarios

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

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

Constraints

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

Procedure

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

Creating a FlexusX Instance Group

Create a FlexusX instance group, so that you can apply a policy to the entire group. FlexusX instance groups are independent from each other.

1. Access the page for creating a FlexusX instance group from the ECS console or the FlexusX console as follows:

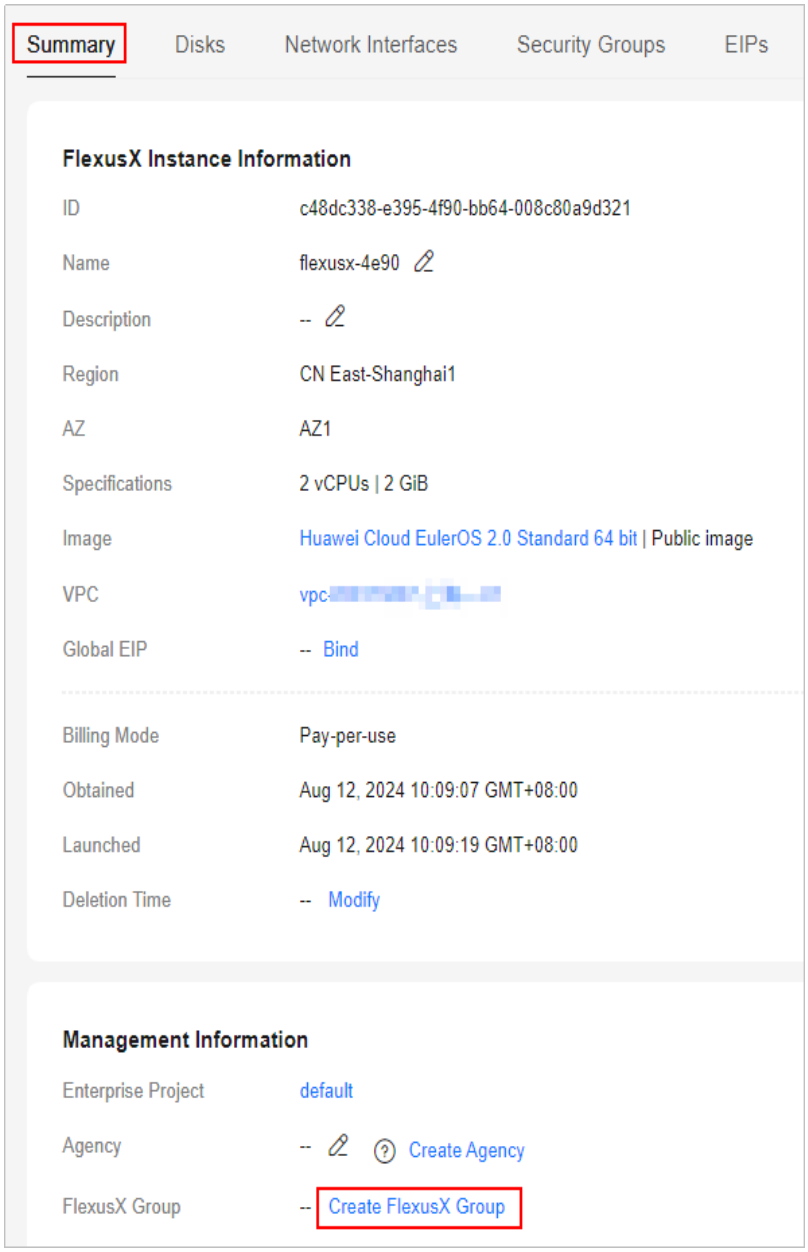
   NOTE

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

   - Log in to the **ECS console**. Switch to the **ECS Group** page, click  in the upper left corner, and select a region.
   - Log in to the FlexusX **console**, in the upper left corner, click  , and select a region.

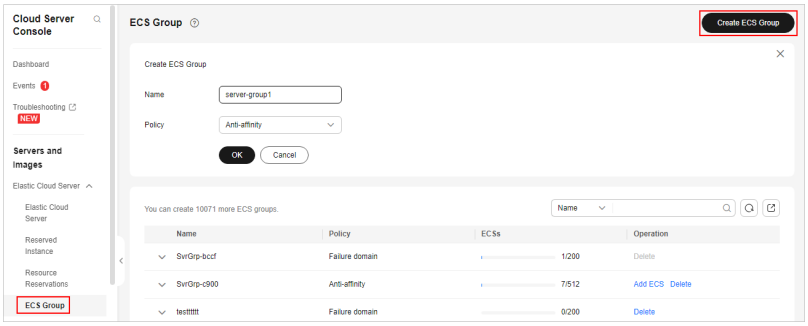
Click the name of a FlexusX instance. On the details page, click **Create FlexusX Instance Group**.

Figure 4-12 Creating a server group



2. On the **ECS Group** page, click **Create ECS Group** and set the ECS group name and policy.

   Only the anti-affinity policy is supported.



3. Click **OK**.

Adding a FlexusX Instance to a FlexusX Instance Group

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

- You can add a FlexusX instance to a FlexusX instance group when you are creating the instance. For details, see **Step 2: Configure Parameters**.
- You can also add a FlexusX instance to a FlexusX instance group after you create the instance, as described in this part.

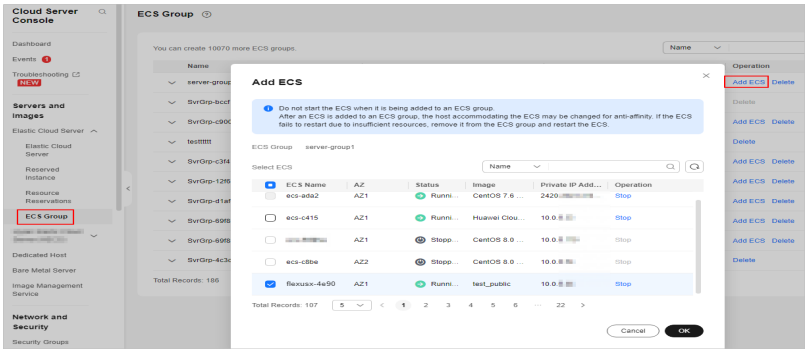
NOTE

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

1. Log in to the **ECS console**. Switch to the **ECS Group** page, click  in the upper left corner, and select a region.
2. Locate the row that contains the target FlexusX instance group and click **Add ECS** in the **Operation** column.

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

Figure 4-13 Adding a FlexusX Instance

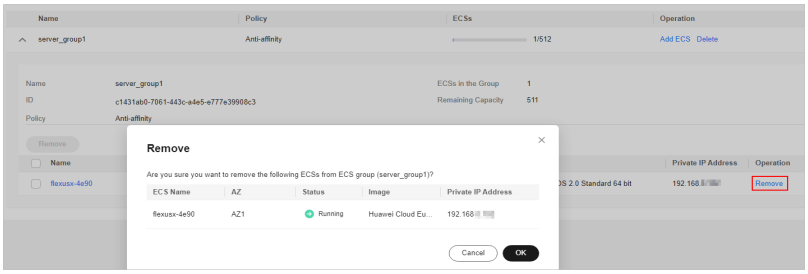


3. Click **OK**.

Removing a FlexusX Instance from a FlexusX Instance Group

If a FlexusX instance is removed from a FlexusX instance group, the anti-affinity policy is no longer applied to that instance.

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



4. Click **OK**.

Deleting a FlexusX Instance Group

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

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

4.6 Viewing Information About a FlexusX Instance

4.6.1 Viewing Details of a FlexusX Instance

Scenarios

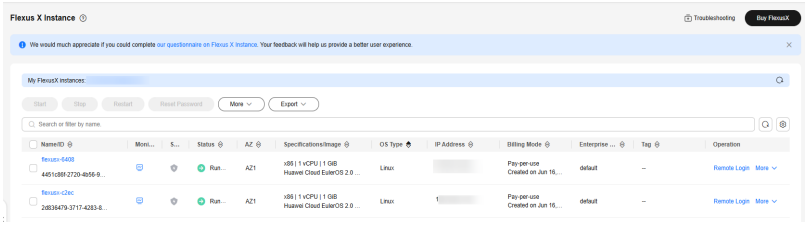
After a FlexusX instance is created, you can view and manage it on the FlexusX instance console. This section describes how to view detailed configurations of a FlexusX instance, including the instance name, image, system disk, data disk, security group, and EIP.

Procedure

1. Log in to the FlexusX **console**, in the upper left corner, click , and select a region.

   On the FlexusX instance list page, you can view the FlexusX instances you purchased and their basic information such as private IP addresses.

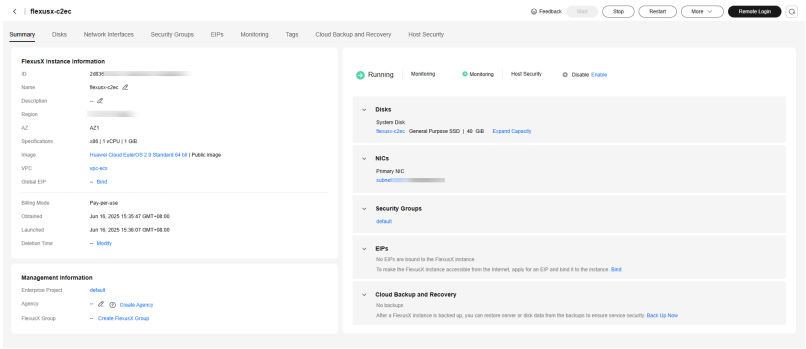
Figure 4-14 List of FlexusX instances



2. (Optional) In the upper part of the list, enter a FlexusX instance name, IP address, or ID and click to search for the FlexusX instance.
3. Click the name of the FlexusX instance.

   The instance details page is displayed.
4. View details of the FlexusX instance.

Figure 4-15 FlexusX instance details page



There are various tabs to choose from, such as **Summary**, **Disks**, **Network Interfaces**, **Security Groups**, and **Monitoring**. Each one displays different basic information for your FlexusX instance. You can review the monitoring data, add disks or NICs, or change the instance's security groups.

Table 4-3 Operations on the instance details page

Tab	Helpful Links
Disks	• Adding an EVS Disk to a FlexusX Instance • Attaching Existing EVS Disks to a FlexusX Instance • Expanding the EVS Disk Capacity of a FlexusX Instance • Detaching an EVS Disk from a FlexusX Instance Online
Network Interfaces	• Attaching Extended Network Interfaces to a FlexusX Instance • Detaching Extended Network Interfaces from a FlexusX Instance • Changing the VPC for a FlexusX Instance

Tab	Helpful Links
Security Groups	• **Configuring Security Group Rules for a FlexusX Instance** • **Changing the Security Group of a FlexusX Instance**
EIPs	• **Binding an EIP to a FlexusX Instance** • **Unbinding an EIP from a FlexusX Instance** • **Modifying the Bandwidth of a FlexusX Instance**
Monitoring	**Viewing Monitoring Metrics of a FlexusX Instance**
Tags	A tag identifies a FlexusX instance. Adding tags to FlexusX instances helps you better identify and manage your FlexusX instances. You can add up to 10 tags to each instance.
Cloud Backup and Recovery	• **Associating a FlexusX Instance with a Backup Vault** • **Backing Up a FlexusX Instance**
Host Security	**Configuring HSS for a FlexusX Instance**

4.6.2 Viewing Details of Failed Tasks

Scenarios

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

Procedure

1. Log in to the FlexusX **console**, in the upper left corner, click , and select a region.

   Failure messages are displayed above the instance list.
2. Click **Failures** to view failed task details.

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

Table 4-4 Task types

Task Type	Description
Creation failures	Failed FlexusX instance creation tasks.
Operation failures	Tasks with failed operations and error codes that help you troubleshoot the failures.

For a failed task, try again. If the failure persists, **submit a service ticket** to get technical support.

5 Managing Images

5.1 Overview

An image is a template that contains an OS or service data. It may also contain proprietary software and application software, such as database software. You can use an image to quickly create FlexusX instances with the same configurations.

Image Types

FlexusX instances can be created from public, private, and shared images.

Image Type	Description
Public images	A public image is a widely used, standard image. It contains an OS and pre-installed public applications and is visible to all users. Public images are very stable and their OSs and any included software have been officially authorized for use. If a public image does not contain the environments or software you need, you can use a public image to create a cloud server and then deploy the required environments or software on the server. You can install applications based on your service requirements. If you are familiar with system and application environment configurations, select a public image. FlexusX instances can be created using the following public images: Huawei Cloud EulerOS, CentOS, SUSE, Ubuntu, EulerOS, Debian, OpenSUSE, Fedora, AlmaLinux, Rocky Linux, CentOS Stream, CoreOS, openEuler, FreeBSD, and SUSESAP. **NOTE** • FlexusX instances that use the Huawei Cloud EulerOS 2.0 public image support Nginx, Redis, or MySQL, PostgreSQL or Memcached application acceleration. For more information, see **Configuring Application Acceleration for a FlexusX Instance**. • Images vary depending on regions. Obtain the supported images on the console.
Private images	A private image is created by yourself. A private image can be a system disk image, data disk image, or full-server image. • A system disk image contains an OS and preinstalled software for various services. You can use a system disk image to create a cloud server and migrate your services to the cloud. • A data disk image contains only service data. You can use a data disk image to create EVS disks and use them to migrate your service data to the cloud. • A full-server image contains an OS, pre-installed application software, and service data. It is created using differential backups and the creation takes less time than creating a system or data disk image that has the same disk capacity. You can use a private image to quickly create FlexusX instances with the same configurations as the private image, eliminating the need to configure multiple FlexusX instances repeatedly. For more information, see **Creating a FlexusX Instance from a Private Image or Using a Private Image to Change the OS**.
Shared images	A shared image is a private image shared by another user with you. For more information, see **Sharing Images**.

Related Operations

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

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

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

Operation	Description	Reference
Creating a private image	You can use a FlexusX instance to create a private image. After the image is created, you can use it to create multiple FlexusX instances with the same configurations or to create other cloud servers.	• Creating a System Disk Image • Creating a Data Disk Image • Creating a Full-Server Image
Sharing an image	After creating a private image from a FlexusX instance, you can share the image with other accounts in the same region.	Sharing Images
Replicating an image	After creating a private image from a FlexusX instance, you can: • Use in-region image replication to convert an encrypted image to an unencrypted image, or the other way around. • Replicate the private image to another region and to another account.	• Replicating Images Within a Region • Replicating Images Across Regions
Exporting an image	After a private image is created from a FlexusX instance, you can export it to a standard OBS bucket and then download it to your local PC.	Exporting an Image
Deleting an image	You can delete a private image if you no longer need it.	Deleting Images

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

Scenarios

You can use a private image to quickly create FlexusX instances with the same configurations or change the OS of a FlexusX instance. A private image can be created from a Huawei Cloud server or from an external image file. For more information, see **Image Management Service**.

Billing

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

Constraints

- Images are regional resources. FlexusX instances can only use private images that are in the same region as them.
- Only private images created using x86 servers are supported in FlexusX.
- For Windows private images, FlexusX instances only support Windows Server 2022/2019/2016/2012 R2 Standard Edition and Data Center Edition images purchased from Huawei Cloud KooGallery, as well as Windows private images with the Bring Your Own License (BYOL).
- When you use a private image to create a FlexusX instance or change the OS, ensure that the instance specifications (vCPUs, memory, and system disk capacity) meet the requirements of that private image. Otherwise, the private image cannot be used.

Preparations

First, you need to create a private image based on one of the three scenarios described here.

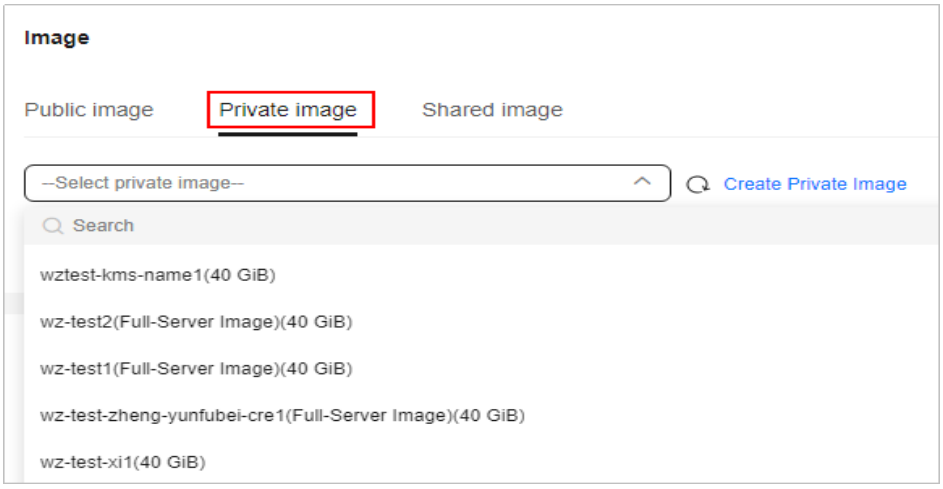
Table 5-1 Creating or importing an image using IMS

Image Source		Reference
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. The import process depends on the image file format. The following formats are supported: • VMDK, VHD, QCOW2, RAW, VHDX, QED, VDI, QCOW, ZVHD2, and ZVHD • ISO	• **Creating a System Disk Image from an External Image File** • **Creating a Linux System Disk Image from an ISO File**
Scenario 3	If you want to use a private image from another account, ask the account owner to share the image with you, and you can replicate the shared image as a private image.	• **Sharing Images** • **Replicating a Shared Image**

Creating a FlexusX Instance from a Private Image

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

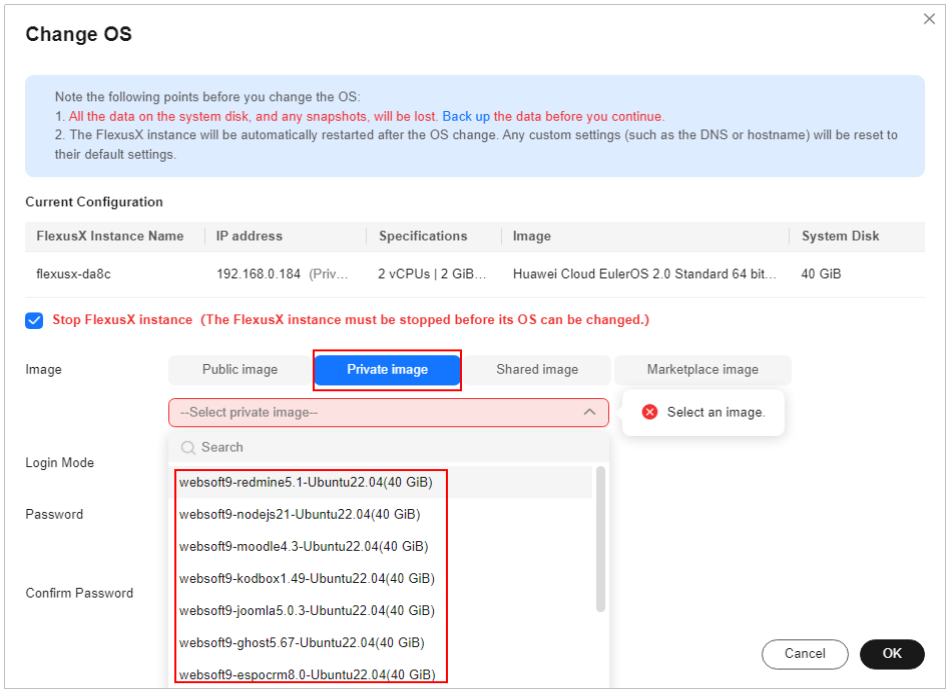
Figure 5-1 Creating a FlexusX instance from a private image



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

After creating or importing a private image using IMS, you can use the private image to change the OS of your FlexusX instance. For details, see **Changing the OS of a FlexusX Instance**.

Figure 5-2 Using a private image to change the OS of a FlexusX instance



5.3 Creating a Private Image from a FlexusX Instance

Scenarios

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

- A system disk image is created from the system disk of a FlexusX instance and contains an OS and application software for running services. You can migrate your services to the cloud using the image.
- A data disk image is created from the data disk of a FlexusX instance and contains only user service data. You can export the data disk of a FlexusX instance by creating a data disk image. You can use a data disk image to create EVS disks and use them to migrate your service data to the cloud.
- A full-server image is created from a FlexusX instance and the data disk of a FlexusX instance and contains user service data. It can be used to quickly provision cloud servers that contain user service data.

You can create a private image on the FlexusX console or the IMS console. This section describes how to create a private image on the FlexusX console.

Billing

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

Constraints

- Only running or stopped FlexusX instances can be used to create private images.
- Do not restart, stop, reset the password of, or reinstall or change the OS of the selected FlexusX instance during image creation.
- A full-server image cannot be created from a FlexusX instance with performance mode enabled.

Procedure

You can create an image from a FlexusX instance on the IMS console. For details, see **Creating a Private Image**.

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

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

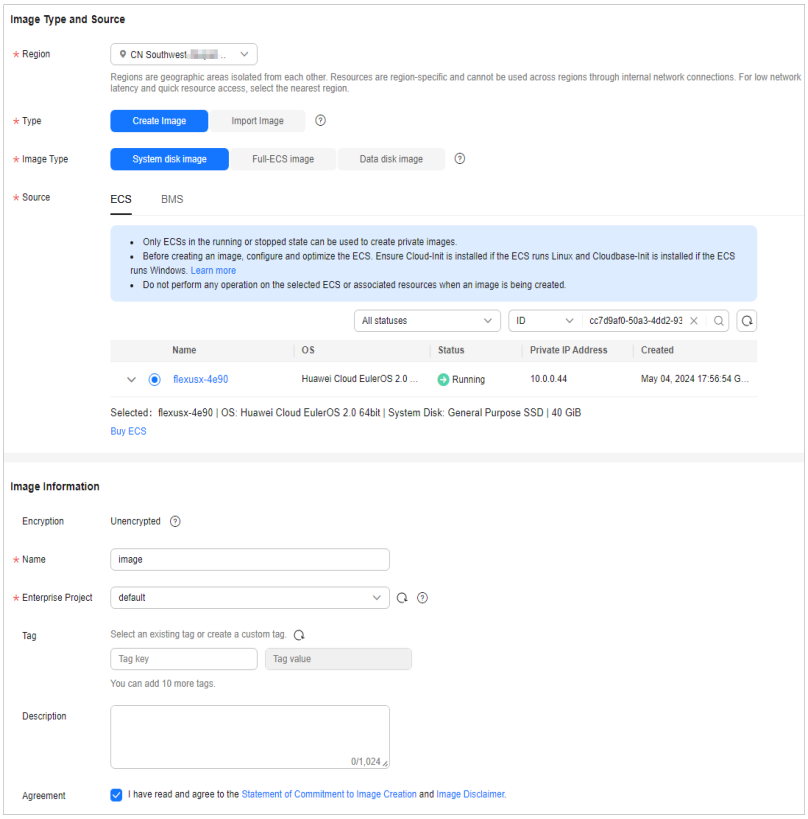


Table 5-2 Image type and source

Parameter	Description
Region	The region where the FlexusX instance is located is preselected. Retain the default value.
Type	Retain the default value **Create Image**.
Image Type	Select an image type from the following: • System disk image • Full-ECS image • Data disk image
Source	• If **Image Type** is set to **System disk image** or **Full-ECS image**, the FlexusX instance from which you want to create an image is selected by default. • If **Image Type** is set to **Data disk image**, select the data disk of the FlexusX instance you want to create an image from.

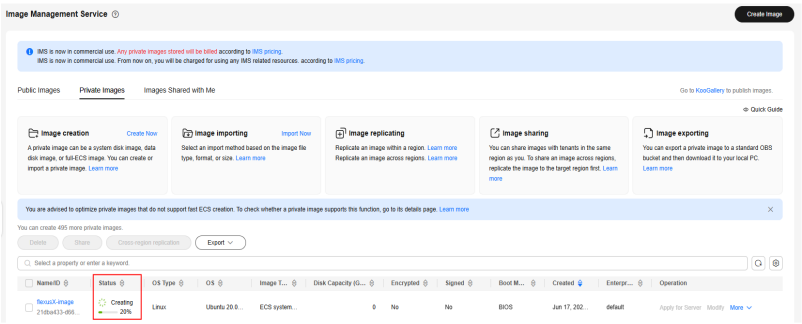
Table 5-3 Image information

Parameter	Description
Encryption	This parameter specifies whether the image will be encrypted. The value is provided by the system and cannot be changed. • Only unencrypted private images can be created from unencrypted FlexusX instances. • Only encrypted private images can be created from encrypted FlexusX instances.
Name	Set a name for the image.
Enterprise Project	Select an enterprise project from the drop-down list. This parameter is only available if you have enabled the enterprise project function, or if your account is an enterprise account. To enable this function, contact your customer manager. An enterprise project provides central management of project resources.
Tag	(Optional) Set a tag key and a tag value for the image to make identification and management of your images easier. For more information about tags, see **Tag Management Service**.
Description	(Optional) Enter a description of the image. It helps you identify and manage the image.

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

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

Figure 5-3 Creating an image



NOTE

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

Helpful Links

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

- Create FlexusX instances. For details, see **Creating a FlexusX Instance from a Private Image or Using a Private Image to Change the OS** or **Creating an ECS from an Image**.
- Change the OS of an existing FlexusX instance. For details, see **Creating a FlexusX Instance from a Private Image or Using a Private Image to Change the OS** or **Changing the OS**.

5.4 Configuring Application Acceleration for a FlexusX Instance

Scenarios

On FlexusX instances created using the **Huawei Cloud EulerOS 2.0** image, certain applications can run at the optimal speed at peak performance thanks to the optimization of the vCPUs, memory, network, storage, kernel, applications, and other settings. Typical applications, such as Nginx, Redis, MySQL, PostgreSQL, and Memcached, can run 10% faster.

When you purchase a FlexusX instance, you need to select the Huawei Cloud EulerOS 2.0 image and then choose an application to be accelerated: Nginx, Redis, MySQL, PostgreSQL, or Memcached. Then the Huawei Cloud EulerOS 2.0 image will pre-install the optimized version of Nginx, Redis, MySQL, PostgreSQL, or Memcached to provide you with the optimal performance. For details about the performance benefits, see **Table 5-4**.

Table 5-4 Performance benefits

Application	Default Version	Performance Benefit	Description
Nginx	1.21.5	• 40% (small HTTP/HTTPS packets) • 15% (large packets)	The enhanced performance results from optimization at the application and OS layers.
MySQL	8.0.40	50% (OLTP read-only, write-only, and mixed read/write)	

Application	Default Version	Performance Benefit	Description
Redis	6.2.7	20% (small single-pipeline packets)	
PostgreSQL	13.18-1	20% (read-only, write-only, and read/write)	
Memcached	1.6.12-2	10% (small single-pipeline packets)	

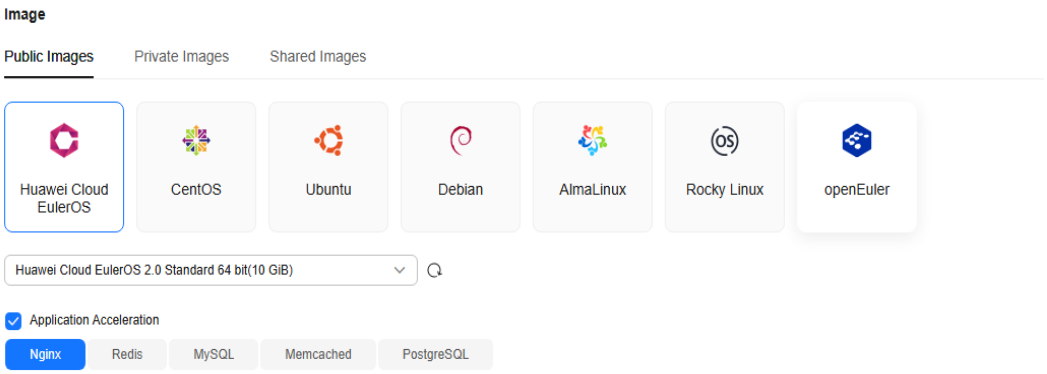
NOTE

- Based on the application acceleration type you configured, the optimized application version from the Huawei Cloud EulerOS yum repository will be installed on the FlexusX instance. If you use other application versions, you may not get the accelerated performance.
- If you choose not to use application acceleration, Nginx, Redis, MySQL, PostgreSQL, and Memcached will not be pre-installed in the Huawei Cloud EulerOS 2.0 image.
- Huawei Cloud EulerOS 2.0 can accelerate only one type of application at a time.
- Huawei Cloud EulerOS 2.0 supports application acceleration only in some regions. For details, see the management console.

Enabling Application Acceleration

When purchasing a FlexusX instance, if you select the **Huawei Cloud EulerOS 2.0** public image, you can enable application acceleration for Nginx, Redis, MySQL, PostgreSQL, and Memcached. For details about how to purchase a FlexusX instance, see **Purchasing a FlexusX Instance**.

Figure 5-4 Setting image information

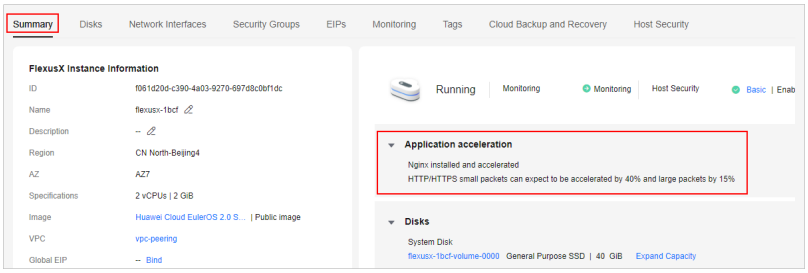


Viewing Application Acceleration

After application acceleration is enabled, the information about the enhanced performance is displayed on the FlexusX instance console. If the application

acceleration information is displayed after you perform the following steps, the application is accelerated:

1. Log in to the FlexusX **console**, in the upper left corner, click , and select a region.
2. Click the name of the FlexusX instance. On the **Summary** tab, view the accelerated application and performance improvement.



Uninstalling the Accelerated Application

If Nginx, Redis, MySQL, PostgreSQL, or Memcached is no longer needed, you can uninstall it. After the application is uninstalled, application acceleration cannot be enabled again.

1. Log in to the FlexusX instance.

   For details, see **Logging In to a FlexusX Instance**.
2. Run the following command as user **root** to uninstall the involved application:

   bash /opt/booster_remove.sh

6 Managing EVS Disks

6.1 Overview

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

System and data disks of FlexusX instances support the following EVS disk types: common I/O, high I/O, General Purpose SSD, ultra-high I/O, and General Purpose SSD V2. By default, a FlexusX instance has a system disk attached. You can configure the type and capacity of the system and data disks based on service requirements. For more information about EVS disk performance, see **Disk Types and Performance**.

Billing

EVS disks are billed based on the disk type, size, and usage duration on a yearly/monthly or pay-per-use basis. For details about EVS billing, see **Billing for EVS Disks**.

Constraints

- When you purchase a FlexusX instance, the EVS disk device type is VBD by default and cannot be changed. After purchasing a FlexusX instance, you can add SCSI data disks.
- When you purchase a FlexusX instance, you can add a maximum of 24 disks (1 system disk and 23 data disks). After purchasing a FlexusX instance, you can add a maximum of 60 disks.

  If more data disks are required, attach them after purchasing a FlexusX instance. To query the number of disks that can be attached to FlexusX instances of different specifications, see **Querying Information About Disks Attached to an ECS**.
- After a new data disk is attached to a FlexusX instance, you need to **initialize the data disk** before using it.

For details about EVS constraints, see **EVS Notes and Constraints**.

Related Operations

Operation	Description
Adding an EVS Disk	• You can purchase data disks when purchasing FlexusX instances, but the disks must be initialized before you can use them. • You can also purchase data disks after purchasing FlexusX instances. – Disks created from data sources, such as backups or snapshots, do not need to be initialized. – Disks that are not created from data sources must be initialized before you can use them.
Attaching an EVS Disk	After a FlexusX instance is created, if the EVS disks on the instance cannot meet service requirements, you can attach existing disks to the FlexusX instance.
Detaching an EVS Disk	• If a file system on your system disk is damaged and your FlexusX instance cannot be started, you can detach the system disk and attach it to another FlexusX instance as a data disk. After the file system is fixed, you can attach the disk back to the original FlexusX instance as the system disk. • If you want to move a data disk from one FlexusX instance to another in the same region and AZ, you can detach the data disk and then attach it to that FlexusX instance. • If you no longer need an EVS disk, you can detach and delete it.
Expanding the EVS Disk Capacity	If the disk capacity of your FlexusX instance is not enough, you can expand the capacity.
Initializing a Data Disk	Data disks must be initialized before they can be used, regardless of whether they are created together with FlexusX instances or created separately and attached to the FlexusX instances. An initialized data disk does not need to be initialized again. **NOTE** • System disks do not need to be initialized. • Data disks containing data do not need to be initialized.

6.2 Adding an EVS Disk to a FlexusX Instance

Scenarios

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

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

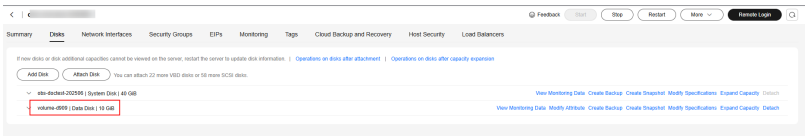
This section describes how to add a data disk after a FlexusX instance is created.

Procedure

1. Log in to the FlexusX **console**. In the upper left corner, click and select a region.
2. Locate the FlexusX instance, and in the **Operation** column, choose **More** > **Manage Disk/Backup** > **Add Disk**.
3. Configure parameters for the new EVS disk as prompted.

   For instructions about how to set EVS disk parameters, see **Purchasing an EVS Disk**.
4. Click **Next** to confirm the order and click **Submit** to complete the payment.
5. Return to the FlexusX console and view the new data disk.

Figure 6-1 Viewing the data disk



Helpful Links

After you add an EVS disk to a FlexusX instance, you still have to log in to the instance and initialize the disk before you can use it. For details about how to initialize a data disk, see **Initializing a Data Disk**.

NOTE

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

6.3 Attaching Existing EVS Disks to a FlexusX Instance

Scenarios

If the disks of a FlexusX instance cannot meet service requirements, for example, there is not enough disk space, you can attach more available disks to the FlexusX instance.

Constraints

- EVS disks can only be attached to FlexusX instances in the same region.
- Non-shared disks can be only attached when they are in the **Available** state.

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

For details about attaching disks, see **Attaching a Non-Shared Disk** and **Attaching a Shared Disk**.

Prerequisites

- EVS disks are available.

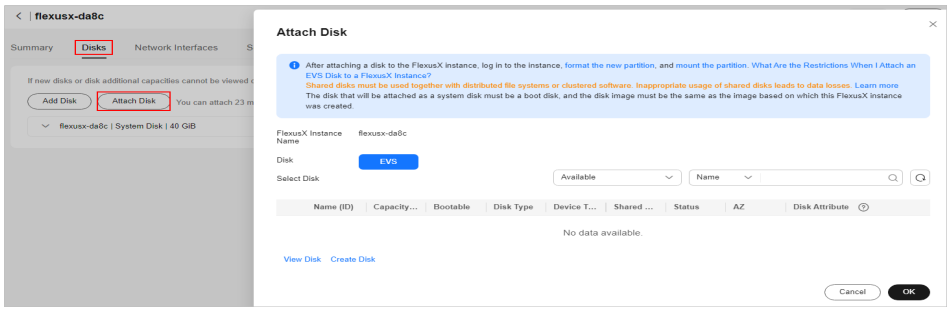
  For instructions about how to purchase an EVS disk, see **Purchasing an EVS Disk**.

Procedure

1. Log in to the FlexusX **console**. In the upper left corner, click  and select a region.
2. Click the name of the FlexusX instance you want to attach a disk to.

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

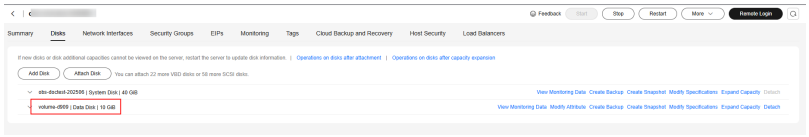
Figure 6-2 Attaching an EVS disk



5. Click **OK**.

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

Figure 6-3 Viewing the data disk



Follow-Up Operations

If the attached disk is newly created, you must log in to the FlexusX instance and initialize the EVS disk before you can use them. For details about how to initialize a data disk, see **Initializing a Data Disk**.

6.4 Expanding the EVS Disk Capacity of a FlexusX Instance

Scenarios

As your business develops or data volume grows, existing EVS disk capacity of a FlexusX instance may no longer meet your storage needs. In this case, you can expand the disk capacity without interrupting your services. Expanding the disk capacity does not affect the data on the disks.

Billing

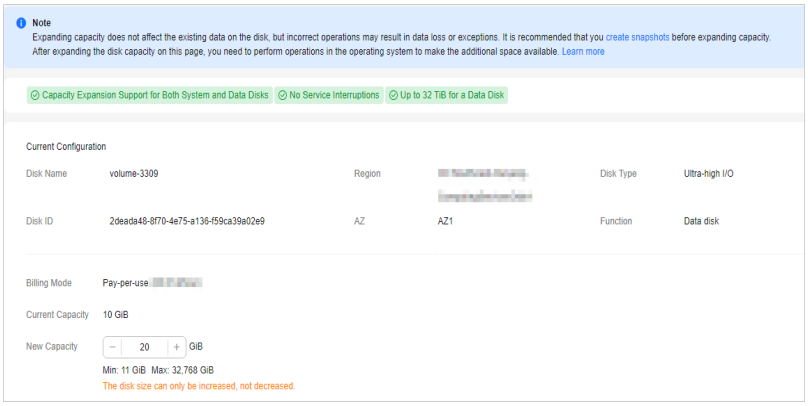
If you scale up an EVS disk, you will be billed for the additional capacity. The billing mode of the additional capacity will be the same as that of the disk.

For details, see **Billing for Disks**.

Procedure

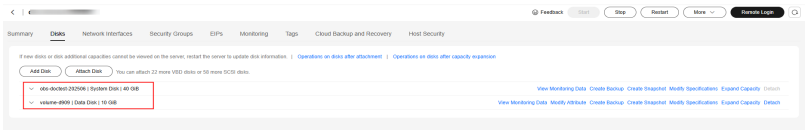
1. Log in to the FlexusX **console**. In the upper left corner, click and select a region.
2. Locate the FlexusX instance, and in the **Operation** column, choose **More** > **Manage Disk/Backup** > **Expand Disk**.

3. Select the disk you want to expand and click **OK**.
4. Set the new capacity of the disk, click **Next**, and follow the on-screen instructions to complete the expansion.



5. Return to the FlexusX console. On the instance details page, view the disk capacity on the **Disks** tab.

Figure 6-4 Viewing the disk capacity



Helpful Links

After the disk capacity is expanded, you have to log in to the FlexusX instance and extend the partition and file system before you can make use of the additional capacity. If the data disk you expanded has not been initialized, you will need to **initialize the disk** after the capacity expansion. There is no need to extend the partition and file system additionally.

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

6.5 Detaching an EVS Disk from a FlexusX Instance Online

Scenarios

You can detach an EVS disk from a FlexusX instance online in any of the following scenarios:

- If a file system on your system disk is damaged and your FlexusX instance cannot be started, you can detach the system disk and attach it to another FlexusX instance as a data disk. After the file system is fixed, you can attach the disk back to the original FlexusX instance as the system disk.
- If you want to move a data disk from one FlexusX instance to another in the same region and AZ, you can detach the data disk and then attach it to that FlexusX instance.

- If you no longer need an EVS disk, you can detach and delete it.

Billing

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

Constraints

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

Prerequisites

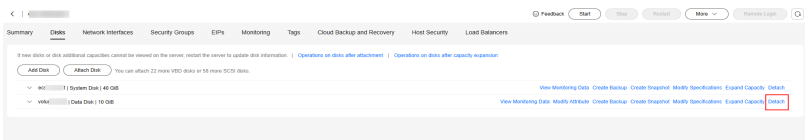
- Before detaching an EVS disk from a running Linux FlexusX instance, you must log in to the instance and use **umount** to cancel the association between the disk and the file system. Also, make sure that there are no programs reading data from or writing data to the disk. Otherwise, you will not be able to detach the disk.
- Detaching and deleting an EVS disk will permanently delete data on it. Back up data before detaching and deleting the disk. You can back up the data by creating EVS snapshots or backing up EVS disks. For details, see **Creating an EVS Snapshot** or **Backing Up EVS Disks**.

Procedure

1. Log in to the FlexusX **console**. In the upper left corner, click and select a region.
2. Click the name of the FlexusX instance that you want to detach a disk from.

   The instance details page is displayed.
3. Click the **Disks** tab. Locate the target disk and click **Detach**.

   Figure 6-5 Detaching the disk



Follow-Up Operations

If you no longer need the detached disk, delete it after backing up the data to prevent the disk from being charged. For details about how to delete an EVS disk, see **Unsubscribing from or Deleting an EVS Disk**.

7 VPC Management

7.1 VPC Overview

VPC

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

The private network communication rules of FlexusX instances are as follows:

- In the same region of an account, multiple FlexusX instances can communicate with each other over a private network only when they are in the same VPC instead of different VPCs.
- FlexusX instances created by different accounts or in different regions are located in different VPCs. They cannot communicate with each other over a private network by default.
- FlexusX instances in the same region can communicate with each other through **VPC Peering Connection**, and those in different regions can communicate with each other through **Cloud Connect**.

For more information about VPC, see **Virtual Private Cloud User Guide**.

Network Interfaces

An elastic network interface (ENI) is a virtual network card. You can create network interfaces and attach them to your FlexusX instances to obtain flexible and highly available network configurations.

There are two types of network interfaces: primary network interfaces and extended network interfaces.

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

Constraints on using network interfaces are as follows:

- The number of network interfaces that can be attached to a FlexusX instance is determined by the instance specifications. For details, see **Instance Specifications**.

  Table 7-1 Constraints on using different types of network interfaces

Network Interface Type	Creation	Attachment	Communication with External Networks	Communication with Public Service Zone
Primary network interface	Created along with the instance by default and cannot be created separately.	Cannot be detached from the instance.	Supported	Supported
Extended network interface	Can be created separately on the **Network Interfaces** page.	Can be attached to or detached from the instance.	Not supported. Policy-based routes need to be configured for external network access. For details about how to configure policy-based routes, see **How Do I Configure Policy-Based Routes for an ECS with Multiple Network Interfaces?**	Not supported

- Extended network interfaces cannot be used to directly access Huawei Cloud services, such as Domain Name Service (DNS). You can use VPC Endpoint (VPCEP) to access these services. For details, see **Buying a VPC Endpoint for Accessing Interface VPC Endpoint Services**.

Billing

In the same region of an account, no additional expenditures are billed for private network access between different FlexusX instances and between FlexusX instances and other Huawei cloud servers in the same VPC. For details about the VPC billing, see **Billing**.

Constraints

When using a VPC, you need to plan VPCs, subnet CIDR blocks, security groups, virtual IP addresses, and elastic NICs. For details about VPC constraints, see **Notes and Constraints**.

Helpful Links

Operation	Description
Attaching Extended Network Interfaces to a FlexusX Instance	If your FlexusX instance requires multiple network interfaces, you can attach extended network interfaces. For details, see **Elastic Network Interface Overview**.
Detaching Extended Network Interfaces from a FlexusX Instance	You can detach extended network interfaces from your FlexusX instance if they are no longer needed. Only extended network interfaces can be detached from the FlexusX instance. You cannot detach the primary network interface from it.
Changing the VPC for a FlexusX Instance	This section describes how to change the VPC of a FlexusX instance.
Changing the Private IP Address of the Primary Network Interface for a FlexusX Instance	You can change the private IP address of the primary network interface for a FlexusX instance on the console.
Configuring a Virtual IP Address for a FlexusX Instance	A virtual IP address serves as a secondary IP address for a network interface. A virtual IP address can be bound to multiple cloud servers to improve server availability.

7.2 Attaching Extended Network Interfaces to a FlexusX Instance

Scenarios

An elastic network interface is a virtual network interface that can be attached to a FlexusX instance in a VPC. You can use network interfaces to manage networks

for FlexusX instances. There are two types of elastic network interfaces: primary network interfaces and extended network interfaces.

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

If your FlexusX instance requires multiple network interfaces, you can attach extended network interfaces. For details, see **Elastic Network Interface Overview**.

Procedure

1. Log in to the FlexusX **console**. In the upper left corner, click and select a region.
2. In the FlexusX instance list, click the name of the FlexusX instance that you want to attach a network interface to.

   The details page of this instance is displayed.
3. On the **Network Interfaces** tab, click **Attach Network Interface**.

   You can use an existing extended network interface or create a new one.

Figure 7-1 Attaching an extended network interface

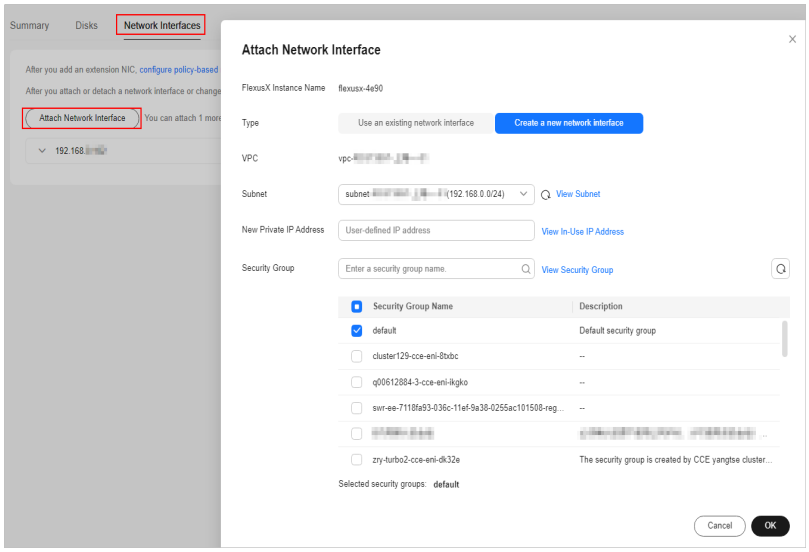


Table 7-2 Parameters for creating a network interface

Parameter	Description
Subnet	This parameter is mandatory. You need to select a subnet where the network interface will work.
New Private IP Address	This parameter is optional. You can specify a private IP address for the network interface. If it is not specified, the system assigns a private IP address automatically.

Parameter	Description
Security Group	This parameter is mandatory. You can select multiple security groups at a time. The rules of all the selected security groups are applied to the FlexusX instance.

4. Click **OK**.

Helpful Links

After an extended network interface is attached to a FlexusX instance, you are advised to enable NIC multi-queue to improve network performance. For details, see **Enabling NIC Multi-Queue**.

7.3 Detaching Extended Network Interfaces from a FlexusX Instance

Scenarios

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

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

Procedure

1. Log in to the FlexusX **console**. In the upper left corner, click and select a region.
2. In the FlexusX instance list, click the name of the FlexusX instance that you want to detach a network interface from.

   The details page of this instance is displayed.
3. On the **Network Interfaces** tab, choose **More** > **Detach**.

   NOTE

   You are not allowed to delete the primary network interface from this instance. By default, the primary network interface is the first one in the list.
4. Click **OK** in the displayed dialog box.

   NOTE

   Some FlexusX instances do not allow to you detach network interfaces while the instances are running. For details, see the on-screen instructions. To detach a network interface from such a FlexusX instance, stop the instance first.

7.4 Changing the VPC for a FlexusX Instance

Scenarios

This section describes how to change the VPC of a FlexusX instance.

The private network communication rules of FlexusX instances are as follows:

- In the same region of an account, multiple FlexusX instances can communicate with each other over a private network only when they are in the same VPC instead of different VPCs.
- FlexusX instances created by different accounts or in different regions are located in different VPCs. They cannot communicate with each other over a private network by default.
- FlexusX instances in the same region can communicate with each other through **VPC Peering Connection**, and those in different regions can communicate with each other through **Cloud Connect**.

Notes

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

  NOTE

  If you intend to change the VPC for a running FlexusX instance when traffic is being routed to the network interface of the instance, the VPC change may fail. In this case, you are advised to try again later or stop the instance and try again.
- After the VPC is changed, the subnet, private IP address, MAC address, and OS network interface name of the FlexusX instance will change accordingly.
- After the VPC is changed, you need to reconfigure the source/destination check and the virtual IP address for the instance.
- After the VPC is changed, you need to reconfigure network-related application software and services, such as ELB, VPN, NAT Gateway, and DNS.

Constraints

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

- If the network interface of a FlexusX instance has an IPv6 address, the VPC cannot be changed for the instance.

Procedure

1. Log in to the FlexusX **console**. In the upper left corner, click and select a region.
2. In the FlexusX instance list, click the name of the FlexusX instance that you want to change the VPC for.

   The details page of this instance is displayed.
3. On the **Network Interfaces** tab, click **Change VPC**.

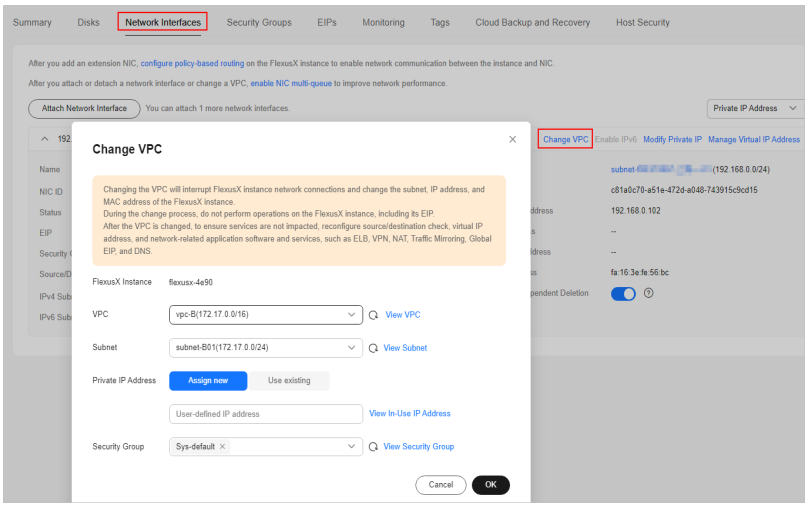
   Select an available VPC and subnet from the drop-down list, and set the private IP address and security group as needed.

   You can select multiple security groups. In this case, the access rules of all the selected security groups are applied to the cloud server.

   NOTE

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

Figure 7-2 Changing a VPC



4. Click **OK**. On the **Network Interfaces** tab, you can check that the VPC has been changed.

7.5 Changing the Private IP Address of the Primary Network Interface for a FlexusX Instance

Scenarios

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

Constraints

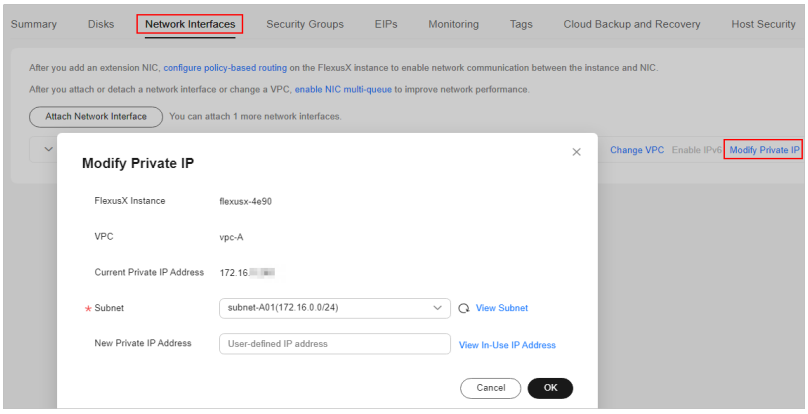
- The FlexusX instance must be stopped.
- If a virtual IP address or DNAT rule has been configured for the network interface, cancel the configuration before modifying the private IP address.
- If the network interface has an IPv6 address, its private IPv4 or IPv6 address cannot be modified.
- To change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

Procedure

1. Log in to the FlexusX **console**. In the upper left corner, click and select a region.
2. In the FlexusX instance list, click the name of the FlexusX instance whose private IP address is to be changed.

   The details page of this instance is displayed.
3. On the **Network Interfaces** tab, locate the primary network interface and click **Modify Private IP**.

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



4. Change the subnet and private IP address of the primary network interface as required.
   - **Subnet**: Select a subnet. Subnets can be changed only within the same VPC.
   - **New Private IP Address**: Specify a new private IP address. If you do not specify a private IP address, the system will automatically assign one to the primary network interface.

7.6 Configuring a Virtual IP Address for a FlexusX Instance

Scenarios

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

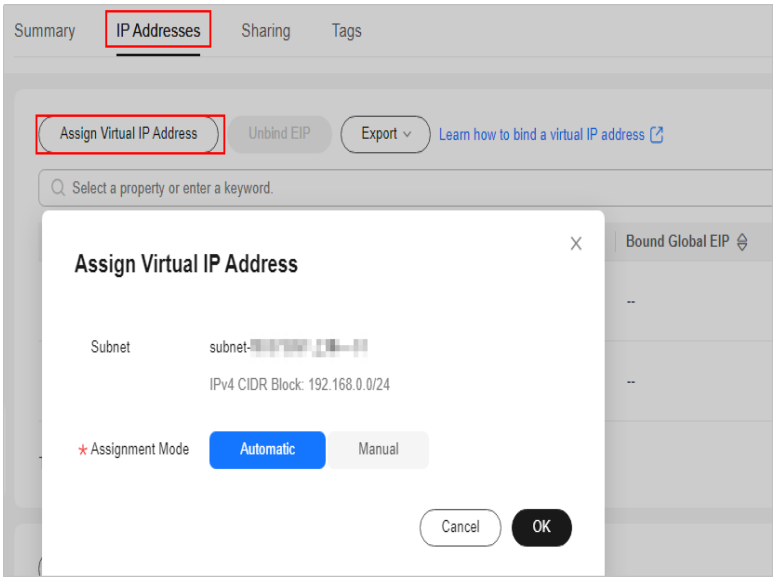
If you want to use a virtual private IP address for a FlexusX instance, apply for a virtual IP address, bind the virtual IP address to the instance, and log in to the instance to manually configure the virtual IP address. This section describes how to use virtual IP addresses. For more information, see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

Procedure

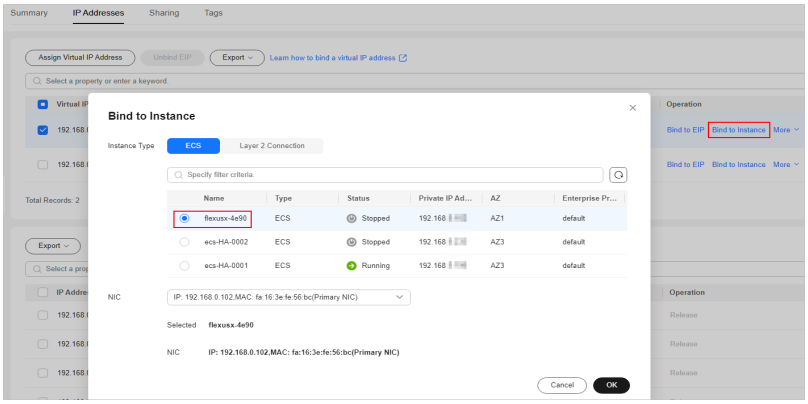
1. Log in to the FlexusX **console**. In the upper left corner, click and select a region.
2. In the FlexusX instance list, click the name of the FlexusX instance that you want to configure a virtual IP address for.

   The details page of this instance is displayed.
3. On the **Network Interfaces** tab, click **Manage Virtual IP Address**.
4. On the **IP Addresses** tab, click **Assign Virtual IP Address**, configure parameters, and click **OK**.

   You can manually set a virtual IP address, or let the system assign one automatically.



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



Follow-Up Operations

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

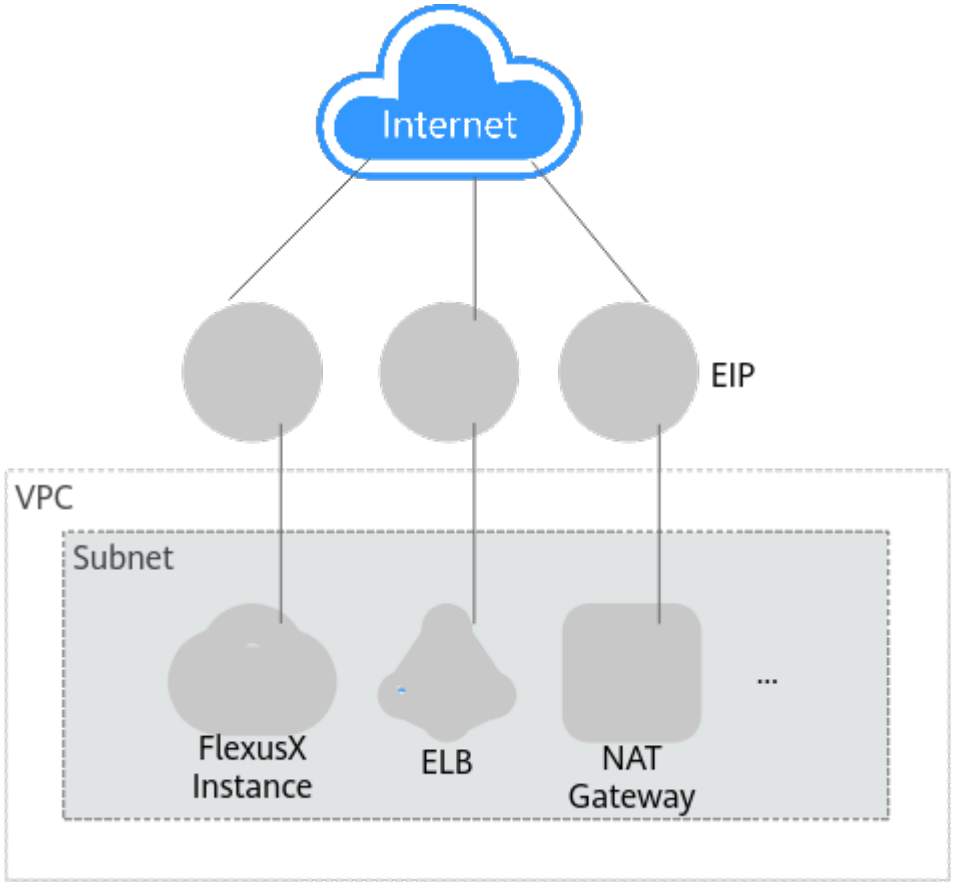
8 Managing EIPs

8.1 Overview

The Elastic IP (EIP) service enables your cloud resources to communicate with the Internet using static public IP addresses and scalable bandwidths. You can easily bind or unbind EIPs to or from FlexusX instances, ECSs, BMSs, virtual IP addresses, NAT gateways, and load balancers as needed. There are different billing modes to meet different service requirements.

If a FlexusX instance has an EIP bound, it can access the Internet. If a FlexusX instance only has a private IP address, it cannot access the Internet. You can purchase an EIP along with a FlexusX instance or purchase an EIP separately on the EIP console and bind it to a FlexusX instance you have purchased.

Figure 8-1 EIP



The EIP used by a FlexusX instance supports the following functions:

- The EIP can be bound to or unbound from the FlexusX instance.
- IPv6 is supported.
- The bandwidth size can be changed.
- If you have released EIPs, the next time you want to bind EIPs, the system preferentially assigns you EIPs from the ones you released in the last 24 hours.

  If you do not want an EIP that you have released, it is recommended that you buy another EIP first and then release the one that you do not need.

For details, see **What Is Elastic IP?**

Billing

- EIPs used by FlexusX instances can be billed on a yearly/monthly or pay-per-use basis.
- EIPs can be billed by bandwidth, traffic, or shared bandwidth.

Constraints

- If a FlexusX instance needs to access the Internet, bind an EIP to the instance.
- EIPs are regional resources. It cannot be used across regions or accounts. Each EIP can be used by only one FlexusX instance at a time, and they must be in the same region.

For more EIP constraints, see **Notes and Constraints**.

Related Operations

Operation	Description	Helpful Links
Binding an EIP	You can bind an EIP to a FlexusX instance so that the instance can access the Internet.	**Binding an EIP**
Unbinding an EIP	If your FlexusX instance does not need to access the Internet or you want to change an EIP, you can unbind the EIP from the instance.	**Unbinding an EIP**
Changing an EIP	You cannot directly change the EIP of a FlexusX instance. To change the EIP, you can unbind the exiting EIP and bind a new one to the instance.	• **Unbinding an EIP** • **Binding an EIP**
Modifying a bandwidth	You can modify the name, billing mode, and size of a bandwidth.	**Modifying a bandwidth**
Releasing an EIP	After an EIP is unbound, it is still billed. If you no longer need the EIP, release it in a timely manner.	**Releasing an EIP**

8.2 Binding an EIP to a FlexusX Instance

Scenarios

If a FlexusX instance needs to be accessed from the Internet, you can apply for an EIP and bind it to the instance.

This section describes how to bind an EIP to a FlexusX instance.

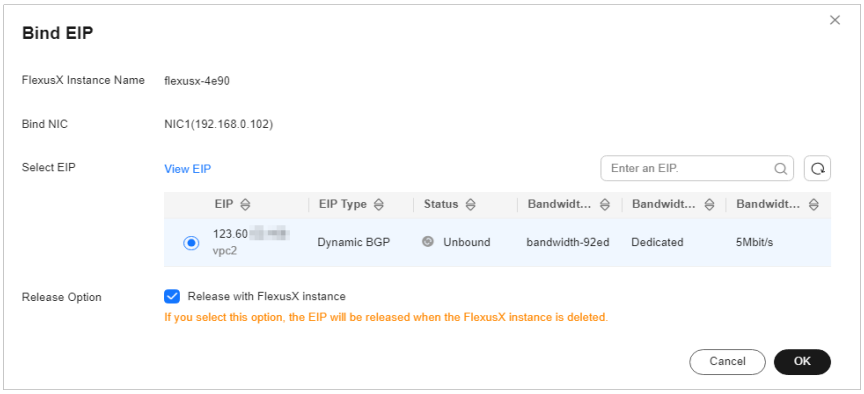
Prerequisites

You have applied for an EIP. For details, see **Assigning an EIP**.

Procedure

1. Log in to the FlexusX **console**. In the upper left corner, click  and select a region.
2. Locate the target FlexusX instance, and in the **Operation** column, choose **More** > **Manage Network** > **Bind EIP**.
3. Bind an EIP.
   - **Select EIP**: Select an EIP from the list. If there are no EIPs available in the current region, the EIP list is empty. In this case, assign an EIP and bind it to your instance.

- **Release Option**: If you select **Release with FlexusX instance**, the EIP will be released when the FlexusX instance is deleted.



4. Click **OK**.

   After an EIP is bound to the FlexusX instance, you can view the bound EIP.

Figure 8-2 Viewing an EIP

8.3 Unbinding an EIP from a FlexusX Instance

Scenarios

If your FlexusX no longer needs an EIP or you want to bind an EIP to another instance, unbind the EIP from the instance first.

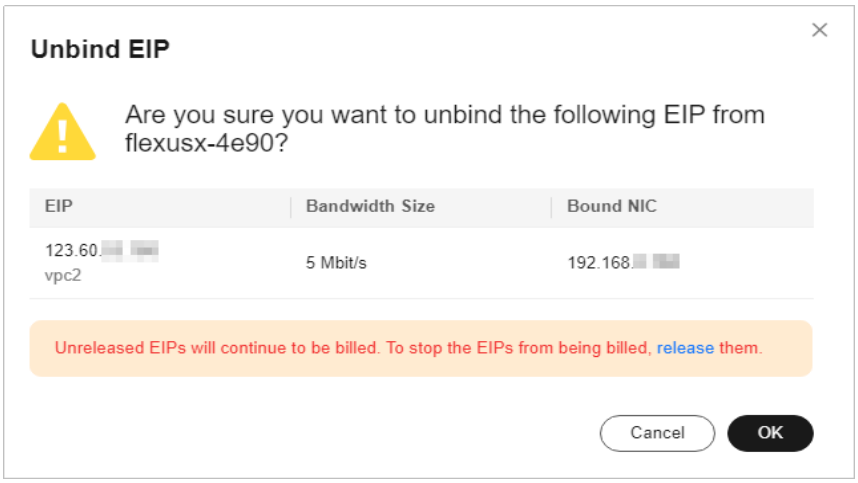
This section describes how to unbind an EIP from a FlexusX instance.

Billing

If you do not release a pay-per-use EIP after unbinding it, it will generate additional costs. If you no longer need it, release it by referring to **Releasing or Unsubscribing From an EIP**.

Procedure

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



NOTE

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

8.4 Modifying the Bandwidth of a FlexusX Instance

Scenarios

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

The rules for modifying EIP bandwidth vary depending on the billing mode of the EIP.

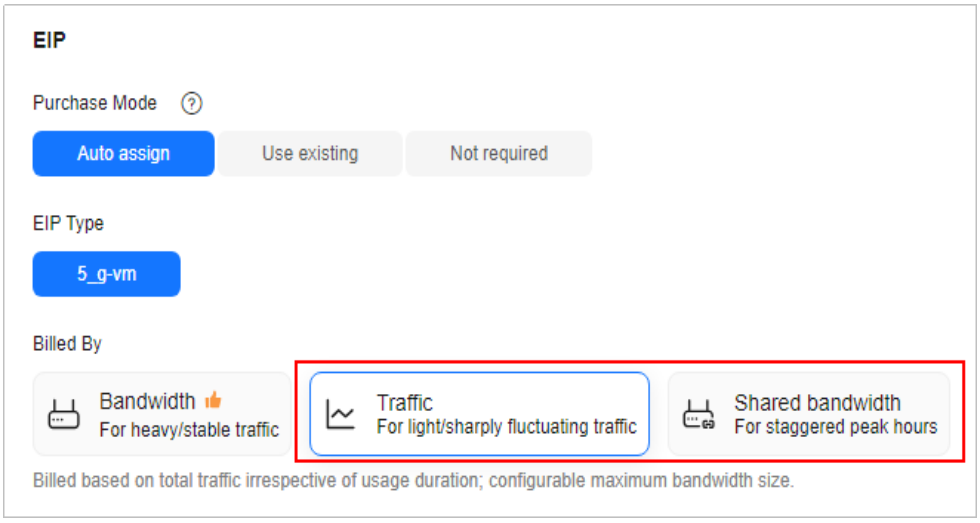
Table 8-1 Rules for modifying the bandwidth of EIPs in different billing modes

EIP Billing Mode	Billing Mode Changeable	Bandwidth Modification	Billing
Yearly/ Monthly	No	• You can only increase the bandwidth in the current subscription period. The modification is applied immediately. • You cannot decrease the bandwidth in the current subscription period. To decrease the bandwidth, **you need to renew the EIP, and the decreased bandwidth will be applied when the next subscription period starts**. Assume you purchased a FlexusX instance with a bandwidth of 5 Mbit/s in March and the subscription period is one month. If you decrease the bandwidth to 2 Mbit/s and renew the EIP for another one month, the bandwidth used in April will be 2 Mbit/s, but the bandwidth used in March is still 5 Mbit/s.	• Increasing bandwidth The increased bandwidth will be billed accordingly. • Decreasing bandwidth The new bandwidth will be billed when the new subscription period starts.
Pay-per-use	Yes	You can increase or decrease the bandwidth. The modifications are applied immediately.	Pay-per-use billing is a postpaid mode, so after the bandwidth is modified, you will be billed based on the new billing mode.

NOTE

- The yearly/monthly and pay-per-use billing modes in **Table 1** define how an EIP is billed, not how the FlexusX instance is billed.

  Yearly/Monthly EIPs can only be billed by bandwidth, but pay-per-use EIPs can be billed by bandwidth, traffic, or shared bandwidth.
- When you purchase a yearly/monthly FlexusX instance, if you select **Traffic** or **Shared bandwidth** for **Billed By**, the EIP is billed on a pay-per-use basis. In this case, use the rules for modifying the bandwidth of a pay-per-use EIP.



Constraints

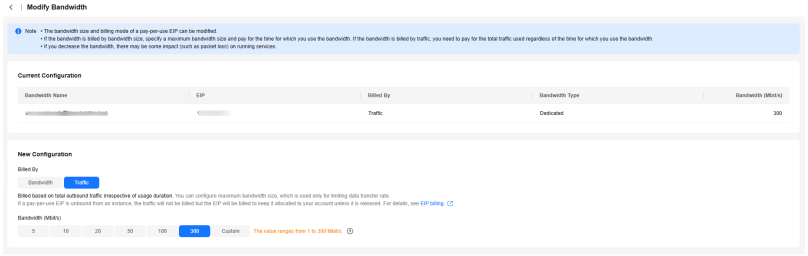
- You can only modify bandwidth for FlexusX instances with EIPs bound.
- If a yearly/monthly EIP is bound to a FlexusX instance:
  - Only the bandwidth name and bandwidth size can be changed. A yearly/monthly EIP can only be billed by bandwidth.
  - The bandwidth size can be increased in the current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

Procedure

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

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

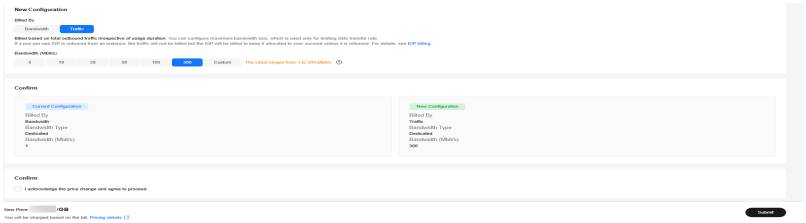
3. Follow the instructions to modify the bandwidth.



Parameter	Description
Billed By	You can select **Bandwidth** or **Traffic** based on service requirements. ● If you choose **Bandwidth**, you will be billed based on the new bandwidth size. ● If you choose **Traffic**, you will be billed based on the total amount of outbound traffic. The bandwidth size you set is only used to limit the maximum transfer rate. **NOTE** A yearly/monthly EIP can only be billed by bandwidth.
Bandwidth (Mbit/s)	● Yearly/Monthly – You can only increase the bandwidth in the current subscription period. The modification is applied immediately. – You cannot decrease the bandwidth in the current subscription period. To decrease the bandwidth, **you need to renew the EIP, and the decreased bandwidth will be applied when the next subscription period starts**. Assume you purchased a FlexusX instance with a bandwidth of 5 Mbit/s in March and the subscription period is one month. If you decrease the bandwidth to 2 Mbit/s and renew the EIP for another one month, the bandwidth used in April will be 2 Mbit/s, but the bandwidth used in March is still 5 Mbit/s. ● Pay-per-use You can increase or decrease the bandwidth. The modifications are applied immediately.

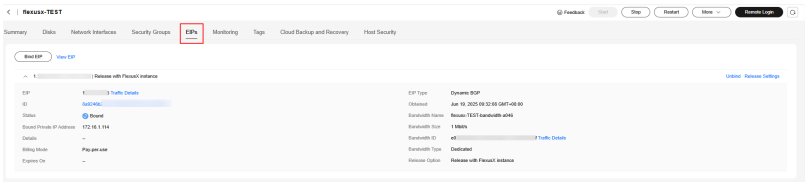
4. Confirm the new configuration, select **I acknowledge the price change and agree to proceed**, and click **Submit**.

Figure 8-3 Confirming the new configuration



5. After the modification is complete, you can view the details on the **EIPs** tab of the FlexusX instance details page.

Figure 8-4 Viewing the bandwidth information



9 Managing Server Security

9.1 Overview

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

Security Protection

FlexusX instances can be protected externally and internally.

Table 9-1 Methods for improving FlexusX 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 FlexusX instances.	• **Enabling HSS** • **Monitoring FlexusX Instances** • **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 when purchasing a FlexusX instance. After the purchase, your instance is automatically protected.
- You can also enable HSS on the HSS console after the FlexusX instance is purchased.

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

Monitoring FlexusX Instances

Monitoring is the key to ensuring FlexusX instance reliability, availability, and performance. Using monitoring data, you can obtain instance resource usage. Cloud Eye collects and displays monitoring data for you in a visualized manner. You can use Cloud Eye to automatically monitor FlexusX instances in real time and manage alarms and notifications, so you can keep track of instance performance metrics.

For more information, see **Cloud Eye Monitoring**.

Backing Up Data Periodically

CBR enables you to back up FlexusX instances and disks with ease. In case of a virus attack, accidental deletion, or software or hardware fault, you can restore data to any point in the past when the data was backed up. CBR protects your services by ensuring the security and accuracy of your data.

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

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

Enhancing the Login Password Strength

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

- The password must consist 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 username/password, such as administrator/administrator, test/test, root/root, oracle/oracle, and mysql/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 9-2 lists some high-risk ports. Do not use these ports for your services.

Table 9-2 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, and 9996
UDP	135 to 139, 1026, 1027, 1028, 1068, 1433, 1434, 4789, 5554, and 9996

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

Periodically Upgrading the OS

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

9.2 Configuring the Security Group for a FlexusX Instance

9.2.1 Overview

Security Group

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.

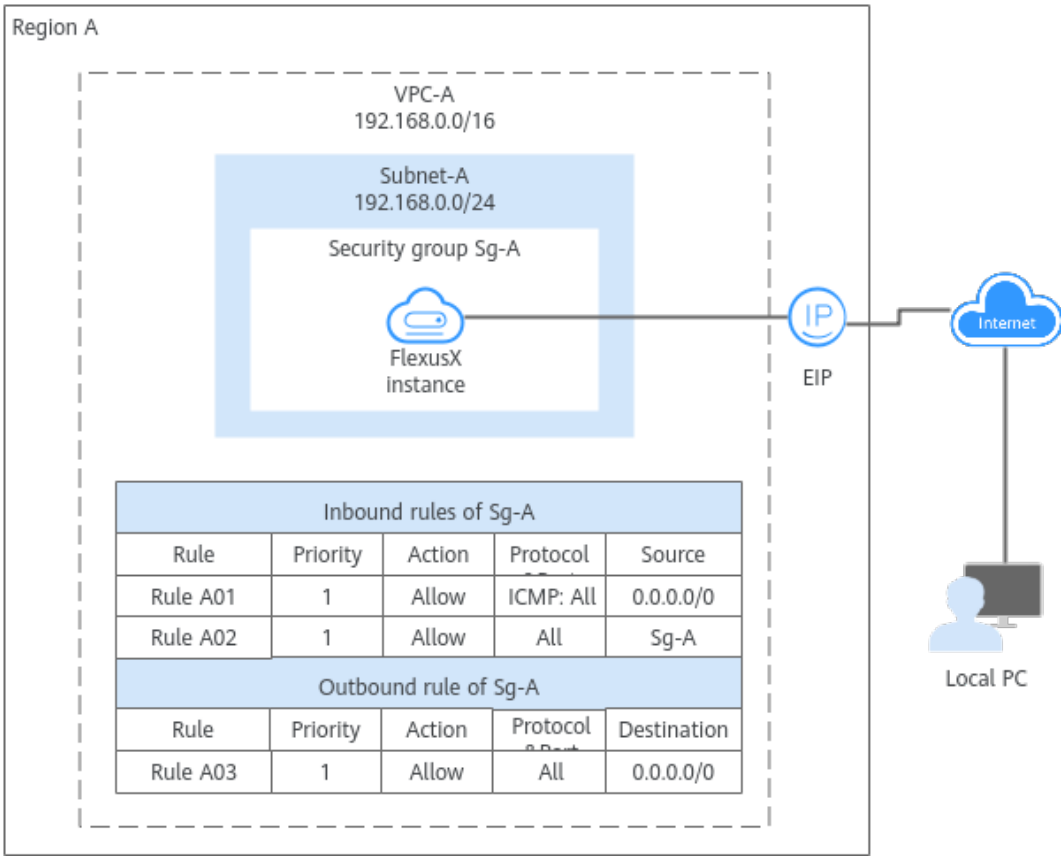
A security group can have inbound and outbound rules. You need to specify the source, port, and protocol for each inbound rule and specify the destination, port, and protocol for each outbound rule to control the inbound and outbound traffic to and from the instances in the security group. As shown in **Figure 9-1**, there is a VPC (**VPC-A**) with a subnet (**Subnet-A**) in region A. A FlexusX instance is running in **Subnet-A** and associated with security group **Sg-A**.

- Security group **Sg-A** has a custom inbound rule to allow ICMP traffic to the 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 FlexusX instance from your PC.

- If the FlexusX instance needs to access the Internet through an EIP, the outbound rule of Sg-A must allow all traffic from the FlexusX instance to the Internet.

Figure 9-1 Security group architecture



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

NOTE

A security group works only when the network communication is normal. If two FlexusX instances are in the same security group but in different VPCs, the instances cannot communicate with each other. To enable communications between the two instances, connect the two VPCs first. For details, see **Connecting VPCs**.

Security Group Rules

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

You can specify the protocol, port, source/destination for a security group rule. The following table describes key parameters about a security group rule.

Table 9-3 Key parameters in a security group rule

Parameter	Description
Priority	The value range is from 1 to 100. A smaller value indicates a higher priority. Security group rules are matched first by priority and then by action. Deny rules take precedence over allow rules.
Action	The action can be **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. • **Protocol**: the protocol that is used to match traffic. The protocol can be TCP, UDP, ICMP, or GRE. • **Port**: the destination port range that is used to match traffic. The value range is from 1 to 65535.
Source/ 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**: an 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. This helps you manage them in an easier way.

You can create a custom security group or use the default one provided by the system. The default security group allows all outbound traffic and denies inbound traffic. FlexusX instances in a security group can communicate with each other without adding any rules.

Table 9-4 Default security group rules

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

Security Group Constraints

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

Helpful Links

Configuring Security Group Rules for a FlexusX Instance

Changing the Security Group of a FlexusX Instance

9.2.2 Configuring Security Group Rules for a FlexusX Instance

Scenarios

Similar to a firewall, a security group is used to control network access. You can define access rules for a security group to protect the FlexusX instances in the group.

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

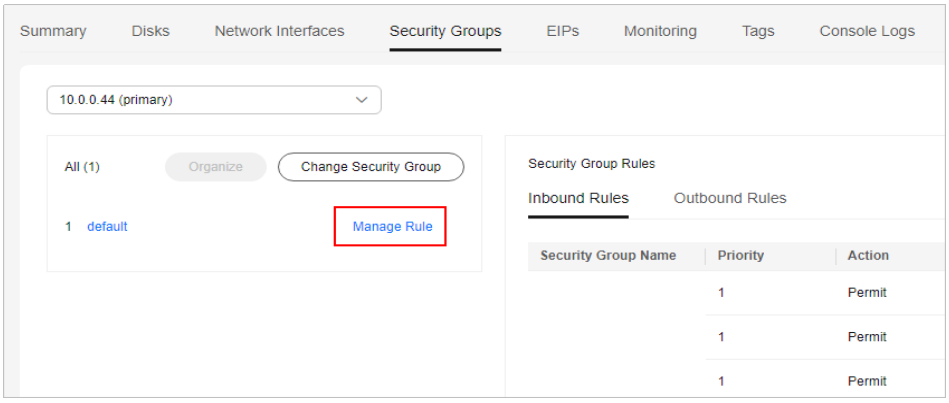
For details about configuration examples, see **Security Group Examples**.

Procedure

1. Log in to the FlexusX **console**. In the upper left corner, click and select a region.
2. On the **FlexusX Instances** page, locate the FlexusX instance and click its name.

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

   The page for configuring security group rules is displayed.

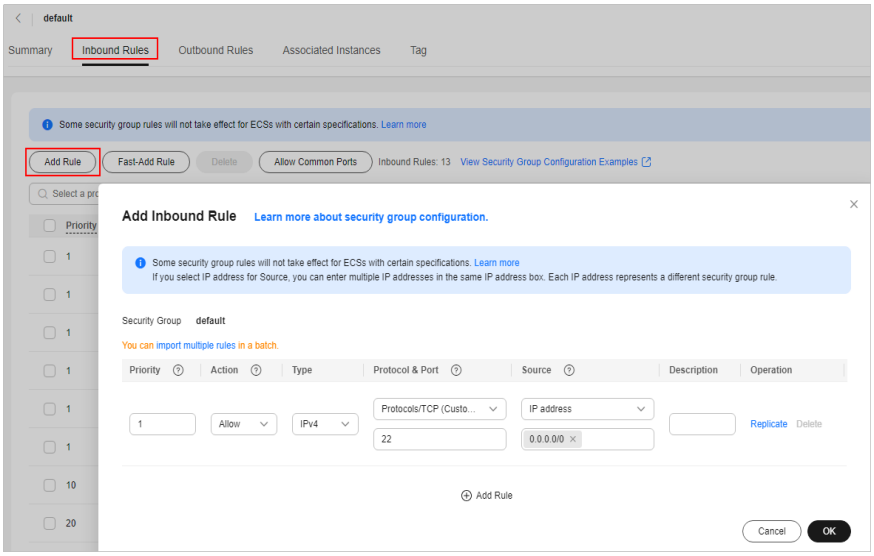


5. On the **Inbound Rules** tab, click **Add Rule**.

   The **Add Inbound Rule** dialog box is displayed.
6. Configure required parameters.

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

Figure 9-2 Adding an inbound rule



7. On the **Outbound Rules** tab, click **Add Rule**.

   The **Add Outbound Rule** dialog box is displayed.

8. Configure required parameters.

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

9. Click **OK**.

   After allowing traffic over a port in a security group rule, you need to ensure that the port used by the instance is also opened. For details, see **Verifying Security Group Rules**.

Impacts of Deleting Common Security Group Rules

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

Deleting security group rules will disable some functions.

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

Helpful Links

- Verifying Security Group Rules
- Why Are My Security Group Rules Not Working?

9.2.3 Changing the Security Group of a FlexusX Instance

Scenarios

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

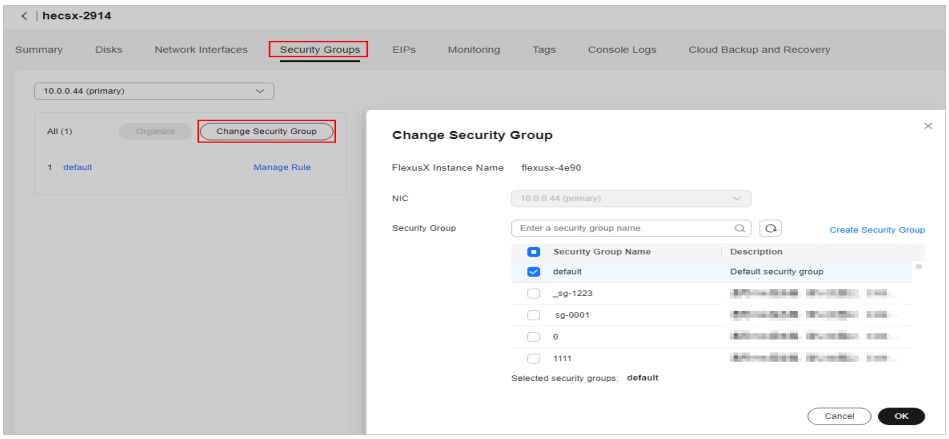
Procedure

1. Log in to the FlexusX **console**. In the upper left corner, click and select a region.
2. On the **FlexusX Instances** page, locate the FlexusX instance and click its name.

   The instance details page is displayed.
3. On the **Security Groups** tab, click **Change Security Group**.

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

   Figure 9-3 Changing a security group



4. Select the network interfaces and security groups.

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

   NOTE

   Using multiple security groups may impact the network performance of a FlexusX instance. You are advised to select no more than five security groups.
5. Click **OK**.

9.3 Configuring HSS for a FlexusX Instance

What Is Host Security Service?

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

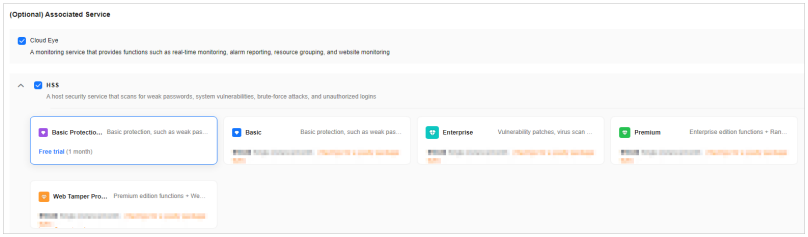
For more information about HSS, see **What Is HSS?**

Enabling HSS

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

  When you use a public image to purchase a FlexusX instance, you can choose to enable HSS. The HSS agent will be installed on and HSS will be enabled for the FlexusX instance automatically.

  Figure 9-4 Enabling HSS during the purchase of a FlexusX instance

  HSS editions:

  – The HSS basic protection trial edition is free for 30 days. It provides functions such as detection for weak passwords, vulnerabilities, brute-force attacks.

    NOTE

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

  – You can choose from the HSS basic, enterprise, premium, and Web Tamper Protection (WTP) editions, which are charged.

    After the instance is purchased, you can switch between different HSS editions on the HSS console. For details about differences among different editions, see **Specifications of Different Editions**.

NOTE

- Whether HSS is displayed on the FlexusX console depends on the selected images. Certain public images do not support HSS.
- The supported HSS editions vary with the billing mode and public image. For details, see the supported HSS editions on the management console.

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

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

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

Viewing the Security Status of FlexusX Instances

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

1. Log in to the FlexusX **console**. In the upper left corner, click  and select a region.
2. In the FlexusX instance list, check the protection status of instances in the **Security** column.

Figure 9-5 Protection statuses

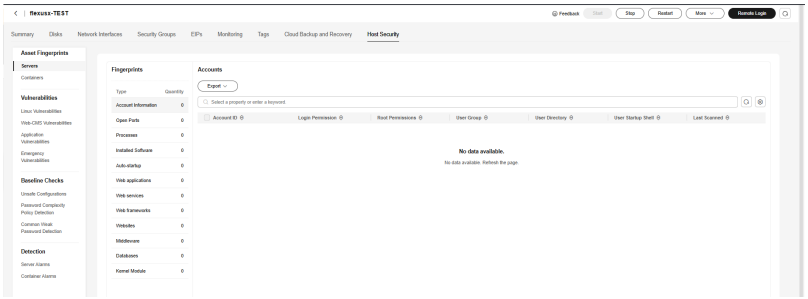
Table 9-5 Protection statuses

Protection Status	Description
Not installed	The agent is not installed, or the agent is installed but not enabled. Click **Learn more** to go to the HSS console and view the agent details. If you want to install the agent, refer to **Installing an Agent**. The security status of a newly purchased FlexusX instance may be **The Agent is not installed**, which is because the agent is currently being installed. Please check the status again later.
Risky	The FlexusX instance is at risk. Click the FlexusX instance name to go to the **Host Security** tab page and view the details.
Safe	No risks have been found in the FlexusX instance.
Unprotected	HSS is not enabled for the FlexusX instance. Click **enable protection immediately** as prompted to go to the HSS console and enable the protection. For details about how to enable HSS, see **Enabling Server Protection**.

3. Click the name of the target FlexusX instance. The details page of this instance is displayed.

Click the **Host Security** tab to view the protection details. For more details, see **What Is HSS?**

Figure 9-6 Host Security tab page



10 Managing Backups

10.1 Overview

What Is CBR?

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 accuracy of your data.

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

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

For more information, see **CBR Architecture**, **Backup Mechanism**, and **Backup Options**.

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

Helpful Links

Operation	Description
Associating a FlexusX Instance with a Backup Vault	If you want to back up a FlexusX instance, associate the instance with a backup vault first.

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

10.2 Associating a FlexusX Instance with a Backup Vault

Scenarios

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

This section describes how to associate an existing FlexusX instance with a new vault.

Billing

See CBR Billing Overview.

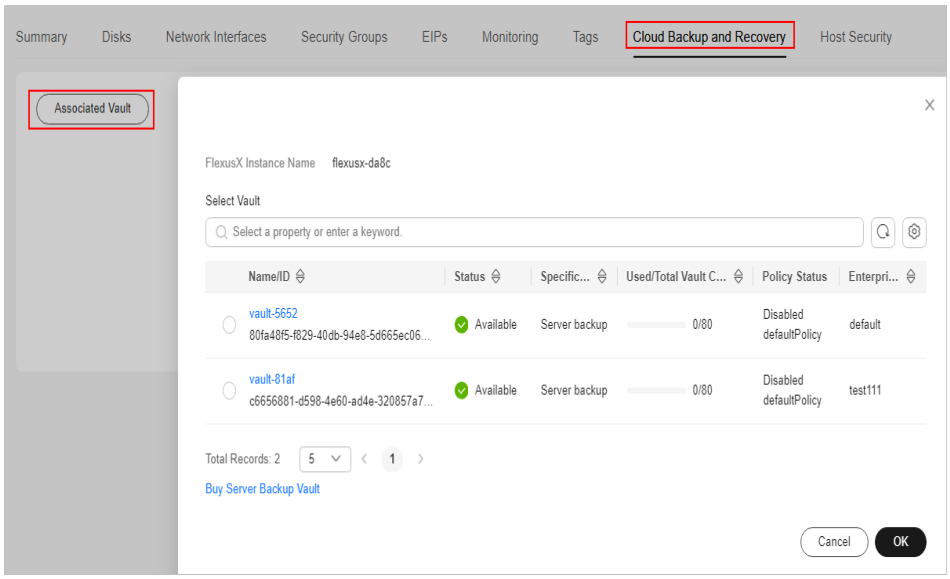
Constraints

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

Procedure

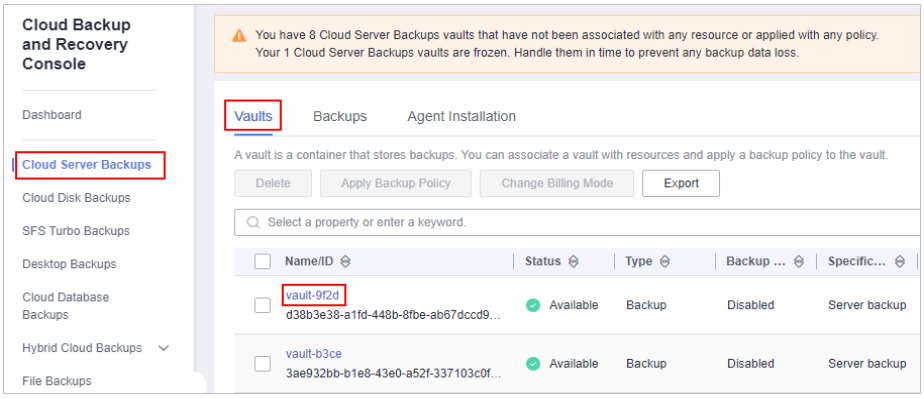
1. Log in to the FlexusX console. In the upper left corner, click and select a region.
2. Locate the FlexusX instance, and in the **Operation** column, choose **More** > **Manage Disk/Backup**.
   - You can click **Create Server Backup** to purchase a server backup vault on the CBR console. For details, see Creating a Server Backup
   - You can click **Create Disk Backup** to purchase a disk backup vault on the CBR console. For details, see Creating a Disk Backup.

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



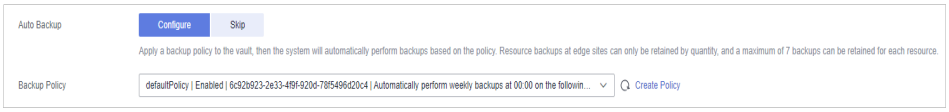
3. View the backup vaults.

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



Helpful Links

- When you are creating a backup vault, you can configure **Auto Backup**, and the system will automatically perform backups based on the policy you configure. You can also manually apply a backup policy to the backup vault. For details, see **Applying a Policy to a Vault**.



- After a backup vault is created, you can also manually back up a FlexusX instance. For details, see **Backing Up a FlexusX Instance**.

10.3 Backing Up a FlexusX Instance

Scenarios

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

For more information, see **CBR Architecture**, **Backup Mechanism**, and **Backup Options**.

Constraints

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

Prerequisites

The FlexusX instance has been associated with a backup vault. For details, see **Associating a FlexusX Instance with a Backup Vault**.

Procedure

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

   NOTE

   If the page for purchasing a backup vault is displayed after you click **Create Server Backup** or **Create Disk Backup**, the FlexusX instance has not been associated with a vault. In this case, **associate the FlexusX instance with a vault** first. Then, create a backup by referring to the steps described in this section.

   – To create a cloud server backup, configure the parameters below.

   Figure 10-1 Creating a cloud server backup

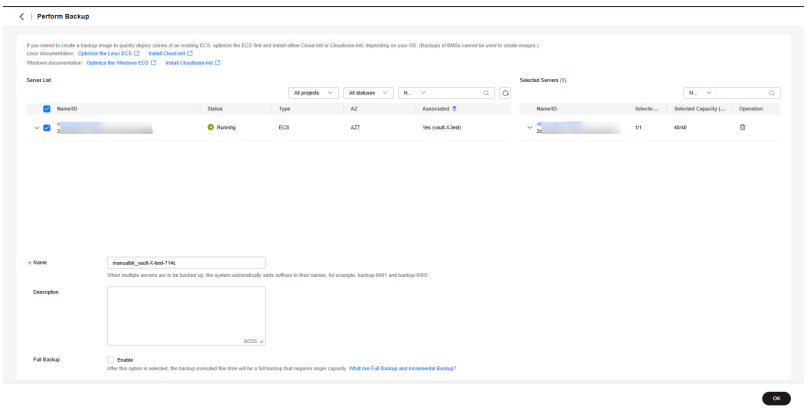


Table 10-1 Parameters for creating a cloud server backup

Parameter	Description
Server List	By default, the cloud servers to be backed up are selected. Click to view the disks attached to the server. Select the disks to be backed up.
Name	Specify your backup name.
Description	Enter a description about the backup.
Full Backup	If you select **Enable**, CBR performs a full backup for each associated server. This requires a larger capacity than an incremental backup.

- To create a cloud disk backup:

  Click **Perform Backup** in the **Operation** column and configure backup parameters as instructed.

Figure 10-2 Performing a backup

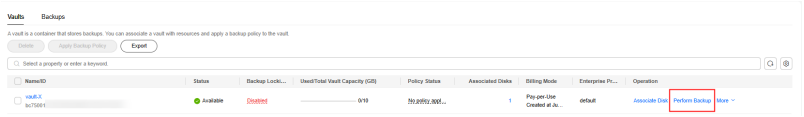


Figure 10-3 Cloud disk backup

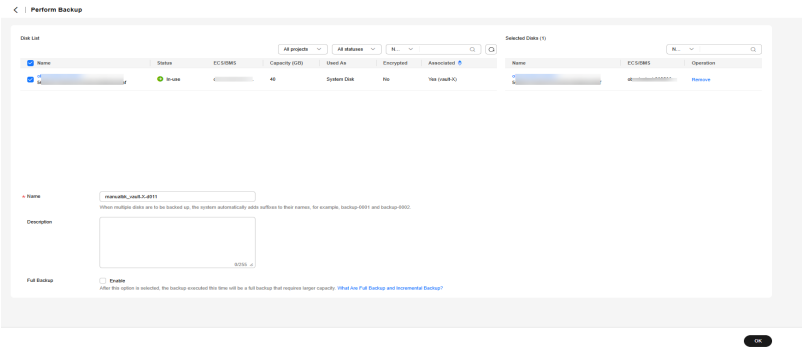


Table 10-2 Parameters for creating a cloud disk backup

Parameter	Description
Disk List	In the disk list, all disks are selected by default. Select the disks to be backed up.
Name	Specify your backup name.
Description	Enter a description about the backup.
Full Backup	If you select **Enable**, CBR performs a full backup on every selected disk. This requires a larger capacity compared to an incremental backup.

3. Click **OK**. The system starts to create a backup immediately.
4. Click **Go to Backup List**.

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

Figure 10-4 Server backup completed

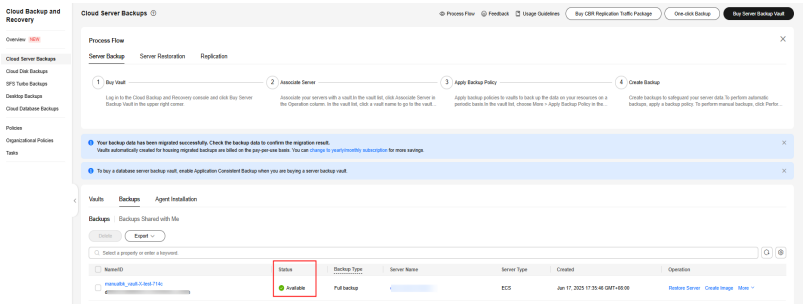
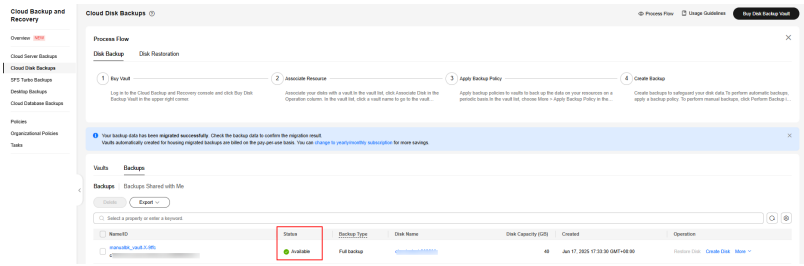


Figure 10-5 Cloud disk backup completed



Helpful Links

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

11 Cloud Eye Monitoring

11.1 Overview

What Is Server Monitoring?

Monitoring is critical to ensuring the reliability, availability, and performance of FlexusX instances. It allows you to view instance resources and learn instance statuses in real time. You can use Cloud Eye to automatically monitor FlexusX instances in real time and manage alarms and notifications. This helps you keep track of performance metrics of FlexusX instances.

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

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

For details about metrics, see **Basic ECS Metrics**, **OS Monitoring Metrics Supported by ECSs with the Agent Installed** and **Process Monitoring Metrics Supported by ECSs with the Agent Installed**.

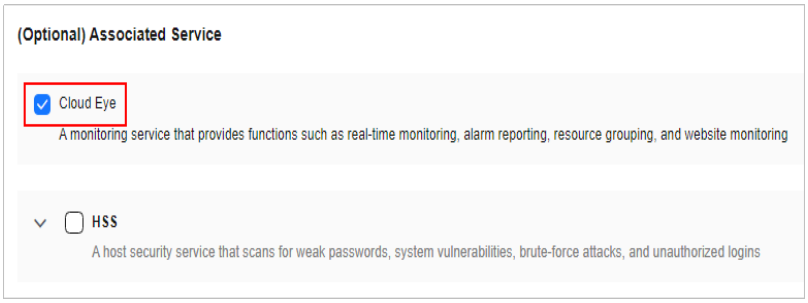
Enabling Monitoring

On the FlexusX instance purchase page, you can choose whether to use Cloud Eye. Regardless of whether you use Cloud Eye or not, after a FlexusX instance is created, basic monitoring is provided for your instance by default. On the FlexusX instance purchase page:

- If you select Cloud Eye, you will be able to view basic monitoring, OS monitoring, and process monitoring data on the FlexusX console. The OS

monitoring and process monitoring data can be viewed only after the **Agent** is installed.

Figure 11-1 Selecting Cloud Eye



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

  If you want to view OS monitoring or process monitoring data, install the **Agent**, and then view the OS monitoring or process monitoring data on the Cloud Eye console.

NOTE

Whether Cloud Eye is displayed on the FlexusX console depends on the selected images. Certain public images do not support Cloud Eye.

Helpful Links

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

11.2 Configuring Alarm Rules for a FlexusX Instance

Scenarios

Configuring alarm rules for FlexusX instances allows you to customize the monitored objects and notification policies. Then, you can monitor your FlexusX instances more carefully.

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

Configuring an Alarm Rule on the Cloud Eye Console

1. Log in to the **Cloud Eye console** and click  in the upper left corner to select a region.
2. In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
3. On the **Alarm Rules** page, click **Create Alarm Rule** to create one, or modify an existing alarm rule. For details, see the following:
   - **Creating an Alarm Rule**
   - **Modifying an Alarm Rule**

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

NOTE

For more information about alarm rules, see **Introduction to Alarm Rules**.

11.3 Viewing Monitoring Metrics of a FlexusX Instance

Scenarios

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

It takes a period of time to transmit and display monitored data. The statuses of FlexusX instances displayed on the Cloud Eye console are obtained 5 to 10 minutes before. You can obtain the monitored data of a newly created FlexusX instance 5–10 minutes later.

Prerequisites

- The FlexusX instance is running properly.

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

  NOTE

  Cloud Eye stops monitoring FlexusX instances that remain in the **Stopped** or **Faulty** state for 24 hours and removes them from the monitoring list. However, the alarm rules configured for such FlexusX instances are not automatically deleted.

- Alarm rules have been configured on Cloud Eye for the FlexusX instance.

  The monitoring data is unavailable for the FlexusX instances without alarm rules configured on Cloud Eye. For details, see **Configuring Alarm Rules for a FlexusX Instance**.

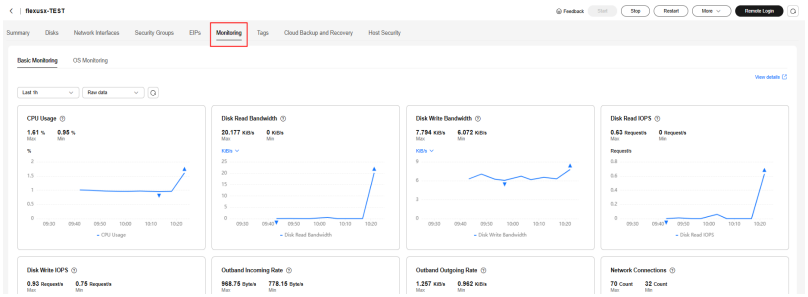
- The FlexusX instance has been running for at least 10 minutes.

  The monitoring data and graphs are not available for a new instance until the instance has been running for at least 10 minutes.

Procedure

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

Figure 11-2 Viewing monitoring details



- 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 1 day.
- 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.
  - **Variance** is the difference between each data point in the original value and the average value within a rollup period.
  - **Sum** is the sum of raw data during a rollup period.

  Rollup is a process where Cloud Eye aggregates the maximum, minimum, average, sum, or variance value of raw data sampled for different periods. This process repeats 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 it based on your service requirements.
- For details about metrics, see **Basic ECS Metrics**, **OS Monitoring Metrics Supported by ECSs with the Agent Installed** and **Process Monitoring Metrics Supported by ECSs with the Agent Installed**.

Helpful Links

- **Why Is My Linux ECS Running Slowly?**

