

Flexus X Instance

User Guide

Issue 01
Date 2024-09-02



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

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

Trademarks and Permissions



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

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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Purchasing a FlexusX Instance.....	1
2 Logging In to a FlexusX Instance.....	8
2.1 Logging In to a FlexusX Instance Using VNC.....	8
3 Managing FlexusX Instances.....	10
3.1 Viewing Details of a FlexusX Instance.....	10
3.2 Resetting the Password for a FlexusX Instance.....	11
3.3 Changing the OS of a FlexusX Instance.....	13
3.3.1 Reinstalling the OS of a FlexusX Instance.....	13
3.3.2 Changing the OS of a FlexusX Instance.....	15
3.4 Modifying the Specifications of a FlexusX Instance.....	17
3.5 Enabling Performance Mode for a FlexusX Instance.....	21
3.6 Managing a FlexusX Instance Group.....	23
3.7 Viewing Details of Failed Tasks.....	26
4 Managing Images.....	28
4.1 Overview.....	28
4.2 Creating a FlexusX Instance from a Private Image or Using a Private Image to Change the OS.....	29
4.3 Creating an Image from a FlexusX Instance.....	32
4.4 Configuring Application Acceleration for a FlexusX Instance.....	35
5 Managing EVS Disks.....	38
5.1 Overview.....	38
5.2 Adding an EVS Disk to a FlexusX Instance.....	39
5.3 Attaching Existing EVS Disks to a Flexus X Instance.....	40
5.4 Expanding the EVS Disk Capacity of a FlexusX Instance.....	41
5.5 Detaching an EVS Disk from a FlexusX Instance Online.....	42
6 Managing Elastic Network Interfaces.....	44
6.1 Overview.....	44
6.2 Attaching Extension Network Interfaces to a FlexusX Instance.....	45
6.3 Detaching Extension Network Interfaces from a FlexusX Instance.....	46
6.4 Changing the VPC for a FlexusX Instance.....	47
6.5 Changing the Private IP Address of the Primary Network Interface for a FlexusX Instance.....	49
6.6 Configuring a Virtual IP Address for a FlexusX Instance.....	50

7 Managing EIPs.....	52
7.1 Overview.....	52
7.2 Binding an EIP to a FlexusX Instance.....	53
7.3 Unbinding an EIP from a FlexusX Instance.....	53
7.4 Modifying the Bandwidth of a FlexusX Instance.....	54
8 Managing Server Security.....	58
8.1 Overview.....	58
8.2 Configuring the Security Group for a FlexusX Instance.....	60
8.2.1 Overview.....	60
8.2.2 Configuring Security Group Rules for a FlexusX Instance.....	61
8.2.3 Changing the Security Group of a FlexusX Instance.....	64
8.3 Configuring HSS for a FlexusX Instance.....	65
9 Managing Backups.....	68
9.1 Overview.....	68
9.2 Associating a FlexusX Instance with Backup Vault.....	69
9.3 Backing Up a FlexusX Instance.....	71
10 Managing Server Monitoring.....	73
10.1 Overview.....	73
10.2 Configuring Alarm Rules for a FlexusX Instance.....	74
10.3 Viewing Monitoring Metrics of a FlexusX Instance.....	75

1 Purchasing a FlexusX Instance


Scenarios

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

Prerequisites

Before purchasing a FlexusX instance, you must have a HUAWEI ID, enable Huawei Cloud services, and add enough money to your account. For more information, see [Preparations](#).

Procedure

1. Log in to the FlexusX [console](#), in the upper left corner, click , and select a region and project.
2. Click **Buy FlexusX**.
3. Select a billing mode.

FlexusX instances support the yearly/monthly and pay-per-use billing modes to meet your requirements in different scenarios. You can change the billing mode from yearly/monthly to pay-per-use, and vice versa. For more information, 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 service.

4. Select a region.

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

Exercise caution when selecting a region. Once a FlexusX instance is created, the region cannot be changed.

5. Select instance specifications.

By default, performance mode is enabled. It can provide ultimate, stable performance assurance at additional costs. For more information, see [Enabling Performance Mode for a FlexusX Instance](#).

You can select either preset or custom FlexusX instance specifications.

6. Select an image.
 - Public images are standard, widely used images. A public image contains an OS and pre-installed public applications. After your instance is created using a public image, you can deploy applications or software on the instance as required.
 - Private images are created on [IMS](#). You can create a private image from a cloud server on Huawei Cloud or another cloud platform, or you can download a third-party image.

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

NOTICE

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

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

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

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

 NOTE

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

- This IP address serves as the start IP address.
 - The required IP addresses must be consecutive and available within the subnet.
 - The subnet that contains the specified IP address cannot overlap with other subnets.
- **IPv6 not required/Automatically-assigned IPv6 address:** This parameter is available only for FlexusX instances of specific flavors in a VPC with IPv6 enabled. For details about how to enable IPv6 on a subnet, see [IPv4 and IPv6 Dual-Stack Network](#). For details about how to check whether a FlexusX instance supports IPv4 and IPv6 dual stack, see "Constraints" in [Dynamically Assigning IPv6 Addresses](#).

By default, the system assigns IPv4 addresses. If you select **Automatically-assigned IPv6 address**, the system assigns IPv6 addresses. In a VPC, a FlexusX instance uses an IPv6 address to access the dual-stack intranet. To access the Internet, you must enable **IPv6 Bandwidth** and select a shared bandwidth. The FlexusX instance then can access the IPv6 Internet through the IPv6 address.

After you create a FlexusX instance, you need to enable IPv6 so that the instance dynamically obtains an IPv6 address. For details, see [Dynamically Assigning IPv6 Addresses](#).

 NOTE

- IPv6 can only be enabled during instance creation. Once enabled, 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.
- c. Set **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.
9. Set EIP parameters.

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.

a. You can select one of the following options:

- **Auto assign:** The system automatically assigns an EIP with a dedicated bandwidth to the FlexusX instance. The bandwidth is configurable.
- **Using existing:** An existing EIP will be assigned to the FlexusX instance. If you select an existing EIP, 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.

b. Set the 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.

c. Set **Billed By**.

This parameter is mandatory when **Purchase Mode** is set to **Auto assign**. If you select **Bandwidth** or **Traffic**, the system will allocate a dedicated bandwidth for you, and the bandwidth is dedicated for one EIP.

- **Bandwidth:** You will be billed based on the amount of bandwidth you configure.
- **Traffic:** You will be billed based on the actual traffic you have used.
- **Shared bandwidth:** You will be billed by the bandwidth shared by multiple EIPs.

d. Set **Bandwidth Size**. Select the bandwidth size (in Mbit/s) based on service requirements.

e. Set **Release Option**. If you select this option, the EIP will be released when the FlexusX instance is deleted.

10. (Optional) Select **Associated Service**.

Enable Cloud Eye or HSS if needed.

- If you enable Cloud Eye, an agent will be automatically installed on your FlexusX instance to provide 1-minute fine-grained monitoring of its metrics, such as vCPUs, memory, network, disks, and processes.
- If you enable HSS, your FlexusX instance will be provided with host security services that scan for weak passwords, system vulnerabilities, brute-force attacks, and unauthorized logins.

There are three HSS editions: basic edition, enterprise edition, and basic protection trial edition. You can use the basic protection trial edition for free for one month. If you do not pay for it after the free trial expires, host security will become unavailable.

11. Set **FlexusX Instance Name** and **Login Mode**.

- a. You can create a custom FlexusX instance name. If you purchase multiple FlexusX instances at a time, the system automatically sequences these instances.
- b. Set **Login Mode**.
 - **Password:** A username and its initial password are used for FlexusX instance login authentication.
 - **Key pair:** A key pair is used for FlexusX instance login authentication. You can select an existing key pair, or click **Create Key Pair** to create a new one.

NOTE

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

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

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

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

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

You can select one of the following options:

- Create new
 - i. Set the name of the cloud backup vault, which consists of 1 to 64 characters, containing only letters, digits, underscores (_), and hyphens (-). For example, **vault-f61e**. The default naming rule is **vault_XXXX**.
 - ii. Enter the vault capacity, which is required for backing up the ECS. The vault capacity cannot be smaller than that of the ECS to be backed up. Its value ranges from the total capacity of the ECS to 10,485,760 in the unit of GB.

- iii. Select a backup policy from the drop-down list, or log in to the CBR console and configure a desired one.
- Use existing
 - i. Select an existing cloud backup vault from the drop-down list.
 - ii. Select a backup policy from the drop-down list, or log in to the CBR console and configure a desired one.
- Not required

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

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

- a. **User Data:** You can inject user data to customize your FlexusX instance. With this configuration, the FlexusX instance automatically injects data the first time it starts up.
 - **As text:** allows you to enter the user data in the text box.
 - **As file:** allows you to inject script files or other files when you create a FlexusX instance.

For example, if you activate user **root** 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](#).

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

NOTE

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

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

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

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

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

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

14. Click **Next: Confirm**.

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

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

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

NOTICE

Back up data before you set the scheduled deletion time.

- Read and agree to the disclaimer.

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

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

Follow-Up Operations

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

 **NOTE**

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

2 Logging In to a FlexusX Instance

2.1 Logging In to a FlexusX Instance Using VNC


Scenarios

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

Prerequisites

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

Procedure

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

```
Huawei Cloud EulerOS 2.0 (x86_64)
Kernel 5.10.0-60.18.0.50.r1083_58.hce2.x86_64 on an x86_64

Hint: Num Lock on

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

        Welcome to Huawei Cloud Service

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



3 Managing FlexusX Instances

3.1 Viewing Details of a FlexusX Instance

Scenarios

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

Procedure

1. Log in to the FlexusX [console](#), in the upper left corner, click , and select a region and project.
On the FlexusX instance list page, you can view the FlexusX instances you purchased and their basic information such as private IP addresses.
2. (Optional) In the upper part of the list, enter a FlexusX instance name, IP address, or ID and click  to search for the FlexusX instance.
3. Click the name of the FlexusX instance.
The details page of this instance is displayed.
4. View details of the FlexusX instance.
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.

3.2 Resetting the Password for a FlexusX Instance

Scenarios

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


Constraints

You can 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 be not 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 and project.
2. Locate the target FlexusX instance, and in the **Operation** column, choose **More > Reset Password**.

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

Figure 3-1 Reset Password

Reset Password ✕

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

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

* New Password

* Confirm Password

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

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

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 after the next restart. Select **Auto Restart**.

NOTE

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

The new password must meet the password complexity requirements.

Table 3-1 Password complexity requirements

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

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

3.3 Changing the OS of a FlexusX Instance

3.3.1 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 and project.
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.

Reinstall OS

Note the following points before you reinstall the OS:

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

[Hide](#)

Current Configuration

HECS X Instance Name	IP address	Specifications	Image	System ...
hecsx-2914	10.0.0.1 (Private IP) 2420:2023:0:0:0:0:0:0	2 vCPUs 2 GiB	Huawei Cloud EulerOS 2.0 Standard 64 bit(64-bit)	40 GiB

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

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

Password:

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

Confirm Password:

[Cancel](#) [OK](#)

4. Click **OK**.
5. On the **Reinstall OS** page, confirm the OS specifications, read and select the agreement or disclaimer, and click **OK**.
After the OS is reinstalled, the FlexusX instance will automatically restart. When the instance status is **Running**, the OS reinstallation is complete.

Follow-Up Operations

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

3.3.2 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 before the system injects the password or key. Otherwise, the login will fail.


Constraints

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

Billing

The new system disk may have a larger capacity after an OS change, so 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 and project.
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.

Change OS

Note the following points before you change the OS:

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

Current Configuration

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

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

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

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

Login Mode: **Password** Key pair

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

Confirm Password: Enter the password again.

Cancel OK

- Click **OK**.
- 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](#).

3.4 Modifying the Specifications of a FlexusX Instance

Scenarios

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

Notes

- Downgrading FlexusX instance specifications (vCPU or memory) will reduce performance.
- The specifications of a FlexusX instance cannot be modified when the instance is in an intermediate state, such as starting, stopping, resetting the OS, or migrating, or when the capacity of EVS disks used by the instance is being expanded.
- 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?](#). This can 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.

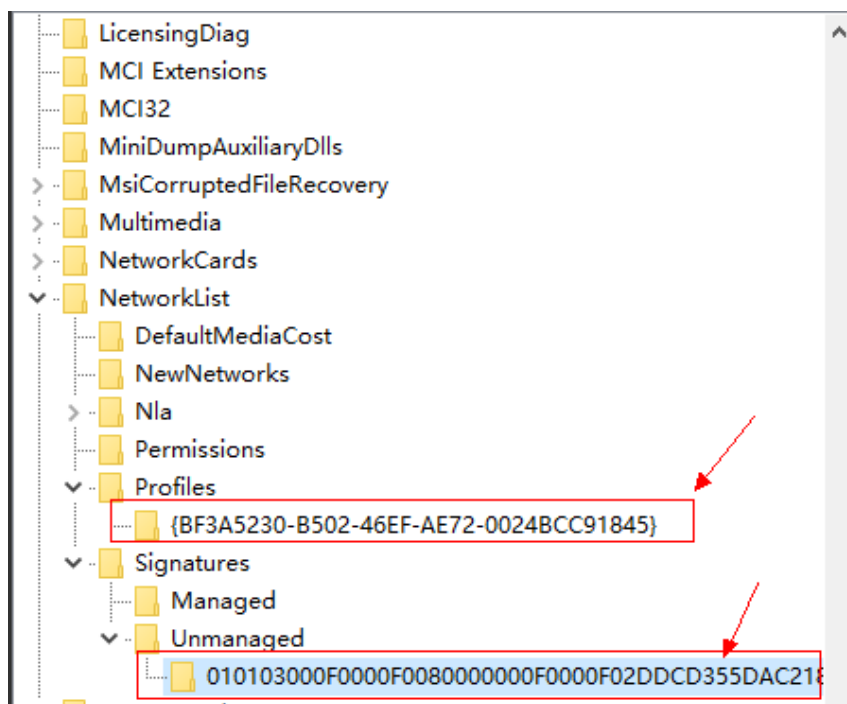
Billing

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 **persistent** and **net** included in their names in 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 in 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 3-2 Registry

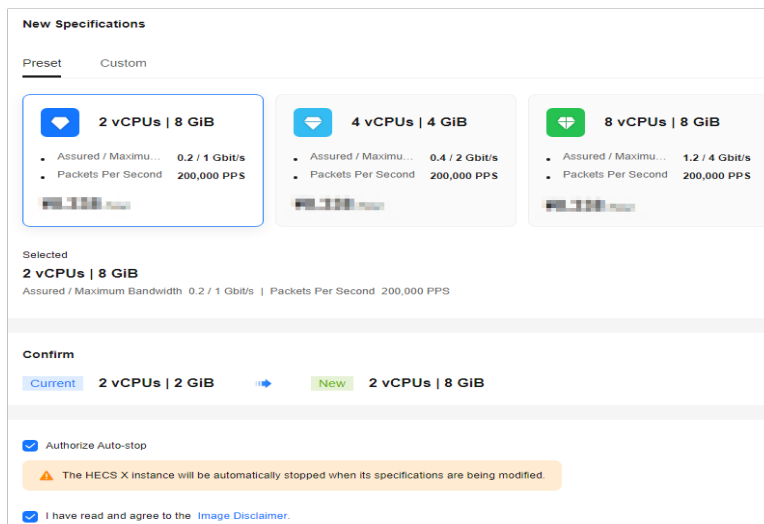
For more information about NIC flapping, see [What Should I Do If NIC Flapping Occurs After My ECS Specifications Are Modified?](#)

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 Specifications of a FlexusX Instance


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



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

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

Batch Modifying Specifications of FlexusX Instances


1. Log in to the FlexusX [console](#), in the upper left corner, click , and select a region and project.
2. Select the Flexus X 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.
 - Select the new specifications.
 - Manually stop the FlexusX instance or select **Authorize Auto-stop**.

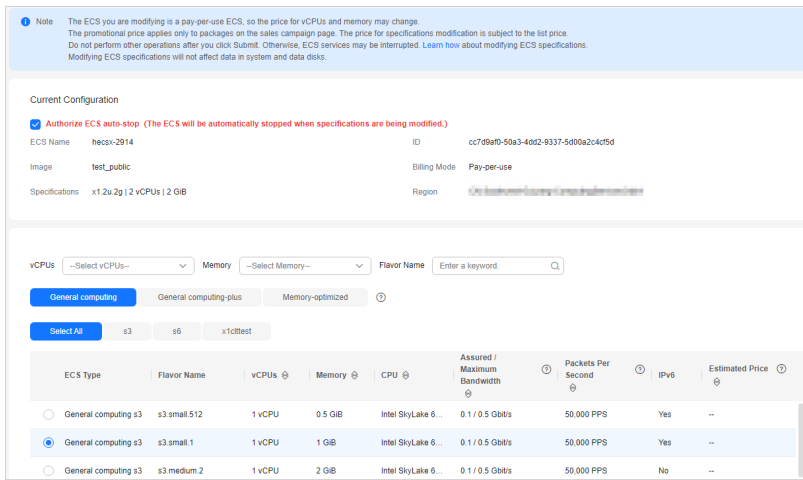


4. Read and agree to the agreement, and click **Submit**.

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

Changing a FlexusX Instance to an ECS

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



Note: The ECS you are modifying is a pay-per-use ECS, so the price for vCPUs and memory may change. The promotional price applies only to packages on the sales campaign page. The price for specifications modification is subject to the list price. Do not perform other operations after you click Submit. Otherwise, ECS services may be interrupted. [Learn how about modifying ECS specifications.](#) Modifying ECS specifications will not affect data in system and data disks.

Current Configuration

Authorize ECS auto-stop (The ECS will be automatically stopped when specifications are being modified.)

ECS Name: hecsx-2914 ID: cc7d9af9-50a3-4d62-9337-5d00a2c4c95d

Image: test_public Billing Mode: Pay-per-use

Specifications: x1.2u.2g | 2 vCPUs | 2 GB Region: [East China \(Hangzhou\)](#)

vCPUs: --Select vCPUs-- Memory: --Select Memory-- Flavor Name: Enter a keyword

General computing | General computing-plus | Memory-optimized

Select All | s3 | s6 | x1c1test

ECS Type	Flavor Name	vCPUs	Memory	CPU	Assured / Maximum Bandwidth	Packets Per Second	IPv6	Estimated Price
<input type="radio"/> General computing s3	s3.small.512	1 vCPU	0.5 GiB	Intel Skylake 6...	0.1 / 0.5 Gbit/s	50,000 PPS	Yes	--
<input checked="" type="radio"/> General computing s3	s3.small.1	1 vCPU	1 GiB	Intel Skylake 6...	0.1 / 0.5 Gbit/s	50,000 PPS	Yes	--
<input type="radio"/> General computing s3	s3.medium.2	1 vCPU	2 GiB	Intel Skylake 6...	0.1 / 0.5 Gbit/s	50,000 PPS	No	--

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

Follow-Up Operations

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

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

3.5 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, ultimate QoS-guaranteed performance.

Additional charges apply to performance mode. [Table 1](#) lists the details about the differences between having performance mode enabled or disabled.

Table 3-2 Differences between having performance mode enabled or disabled

Performance Mode	vCPU Allocation Logic	vCPU Range	Scenarios
Disabled	Flexible compute with QoS-guaranteed performance, close to exclusive instances	1~16	E-commerce going global, enterprise website building, applet development, development and testing, enterprise resource planning (ERP), game servers, and e-commerce livestreaming
Enabled	CPU cores bound to provide QoS-guaranteed ultimate, stable performance	2 to 32	Web 3.0 application development, rendering, cryptocurrency, ERP, game servers, live commerce, e-commerce going global, enterprise website building, applet development, and development and testing

Enabling Performance Mode

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

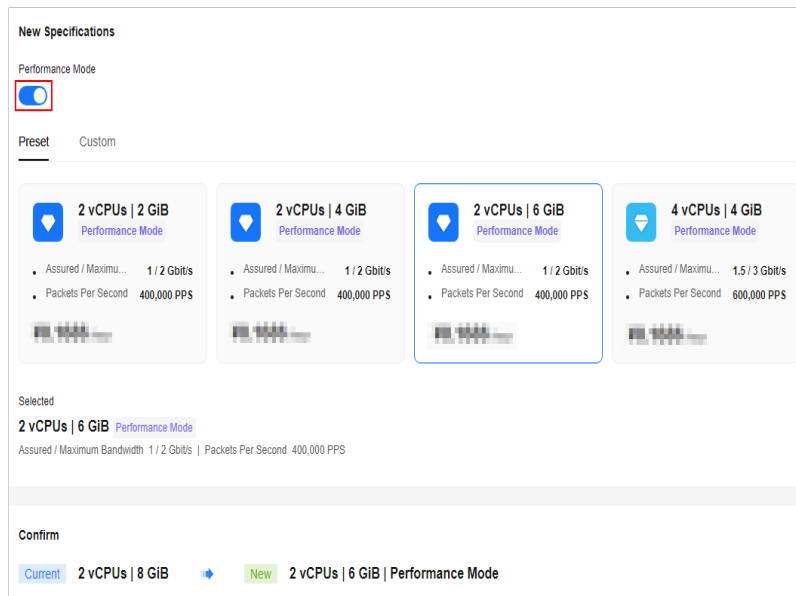
NOTE

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.
- Enabling performance mode after a FlexusX instance is purchased
You can enable the 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](#).

NOTE

Before enabling the performance mode, you need to stop the FlexusX instance.

Figure 3-3 Enabling performance mode using the **Modify Specifications** option

3.6 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.

Supported Operations

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



Creating a FlexusX Instance Group

Create a FlexusX instance group, and 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:

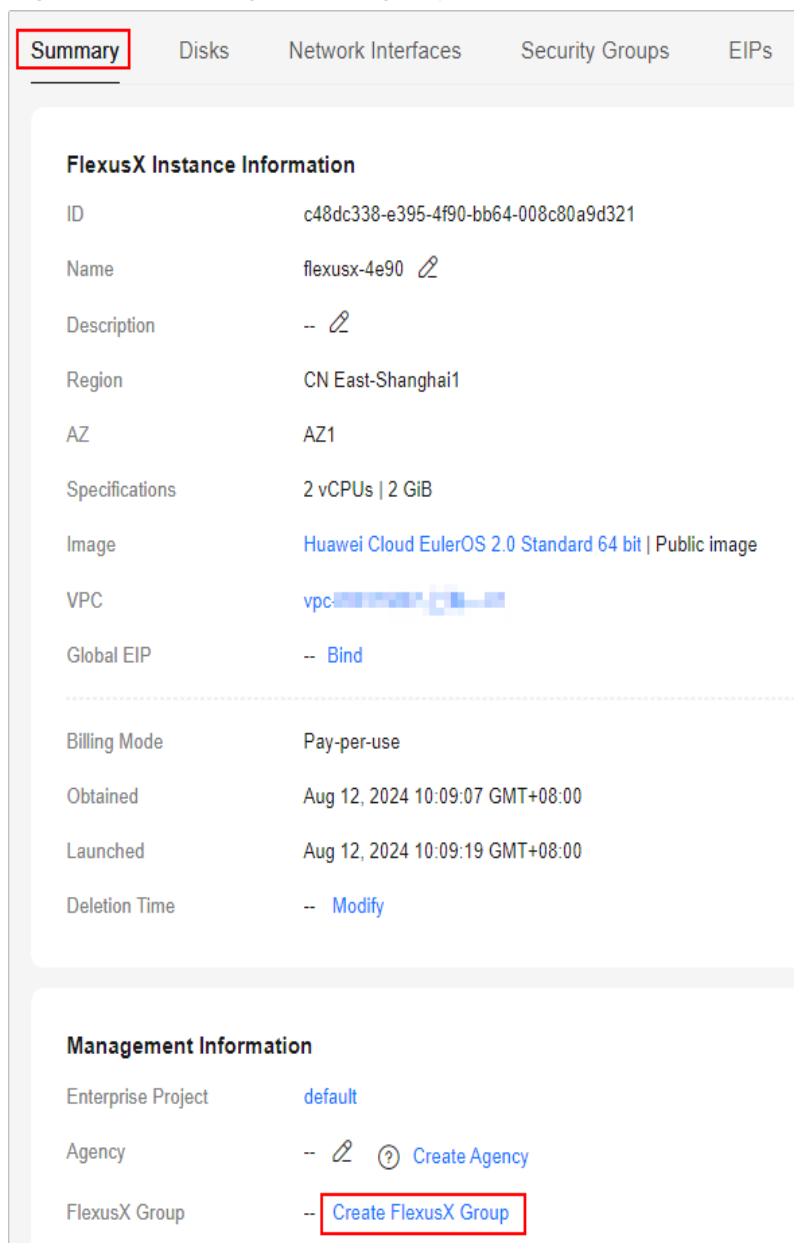
NOTE



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

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

Figure 3-4 Creating a server group

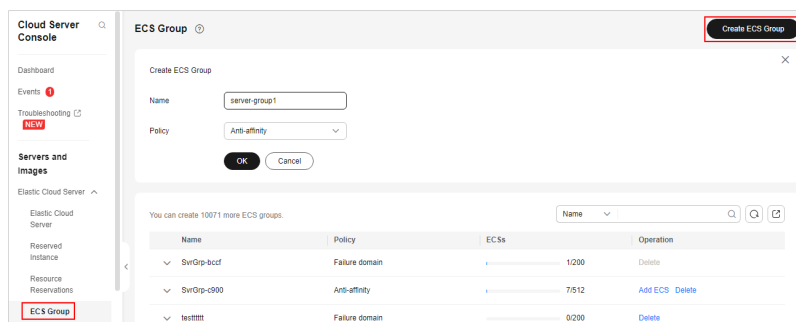


FlexusX Instance Information	
ID	c48dc338-e395-4f90-bb64-008c80a9d321
Name	flexusx-4e90 
Description	-- 
Region	CN East-Shanghai1
AZ	AZ1
Specifications	2 vCPUs 2 GiB
Image	Huawei Cloud EulerOS 2.0 Standard 64 bit Public image
VPC	vpc-...
Global EIP	-- Bind

Billing Mode	Pay-per-use
Obtained	Aug 12, 2024 10:09:07 GMT+08:00
Launched	Aug 12, 2024 10:09:19 GMT+08:00
Deletion Time	-- Modify
Management Information	
Enterprise Project	default
Agency	--   Create Agency
FlexusX Group	-- Create FlexusX Group

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

Only the anti-affinity policy is supported.



3. Click **OK**.


Adding a FlexusX Instance to a FlexusX Instance Group

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

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

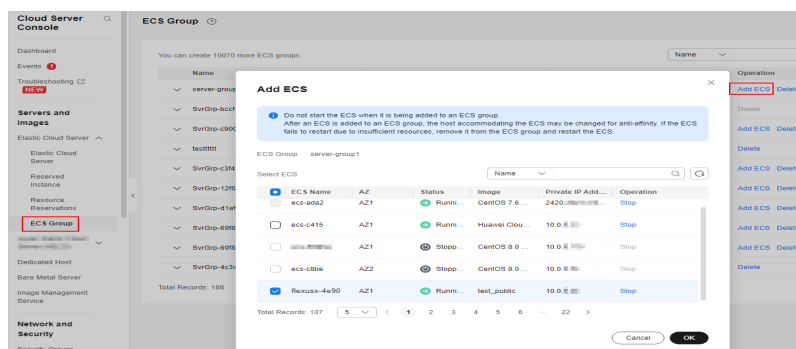
NOTE

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 and project.
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 3-5 Adding a FlexusX Instance

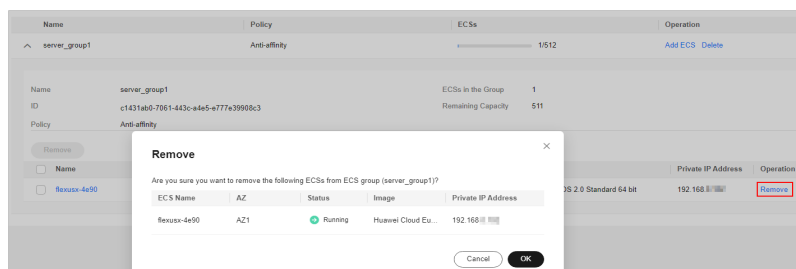


3. Click **OK**.

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 enforced for 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 and project.
2. Expand the FlexusX instance group information and view the FlexusX instances in it.
3. Locate the FlexusX instance to be removed and click **Remove** in the **Operation** column.



4. Click **OK**.

Deleting a FlexusX Instance Group

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


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

3.7 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 and project.
View **Failures** on the right side of buttons for common operations.
2. Click **Failures** to view task details.

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

- **Creation Failures**: the failed FlexusX instance creation tasks

- **Operation Failures:** the tasks with failed operations and error codes that help you troubleshoot the faults

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

4 Managing Images

4.1 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	<p>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 OS 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.</p> <p>You can install applications based on your service requirements. If you are familiar with system and application environment configurations, select a public image.</p>

Image Type	Description
Private images	<p>A private image is created by yourself. A private image can be a system disk image, data disk image, or full-server image.</p> <ul style="list-style-type: none">• 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. <p>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.</p>
Shared images	<p>A shared image is a private image shared by another user with you. For more information, see Sharing Images.</p>

Images Supported by FlexusX Instances

- Public images: Huawei Cloud EulerOS, CentOS, Ubuntu, EulerOS, Debian, openSUSE, AlmaLinux, Rocky Linux, CentOS Stream, CoreOS, openEuler, and FreeBSD
- Shared images and private images of the following types:
 - System disk images, data disk images, and full-server images
 - Linux private images created using x86 servers

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

Scenarios

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

Billing

Creating a FlexusX instance from a private image or using a private image to change the OS does not cost anything.

Constraints

Item	Description
Region	A private image is a regional resource. The FlexusX instances you want to create or change the OS for and the image you want to use must be in the same region. Otherwise, the image cannot be selected.
Cloud server architecture	Only x86 is supported.
Image type	Only Linux images are supported.
Specifications	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 4-1 Creating or importing an image using IMS

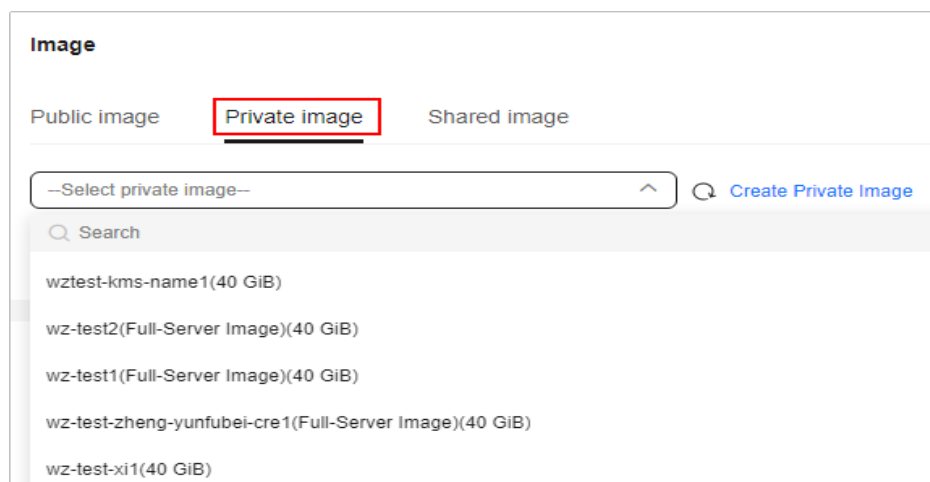
Image Source		Reference
Scenario 1	<p>If your private image is created from a Huawei Cloud ECS or BMS, it can be used in the current region.</p> <p>If you want to use the private image in another region, replicate the image to the region where you want to use it first.</p>	<ul style="list-style-type: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

Image Source		Reference
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.	<ul style="list-style-type: none"> • Sharing Images • Replicating a Shared Image

Creating a FlexusX Instance from a Private Image

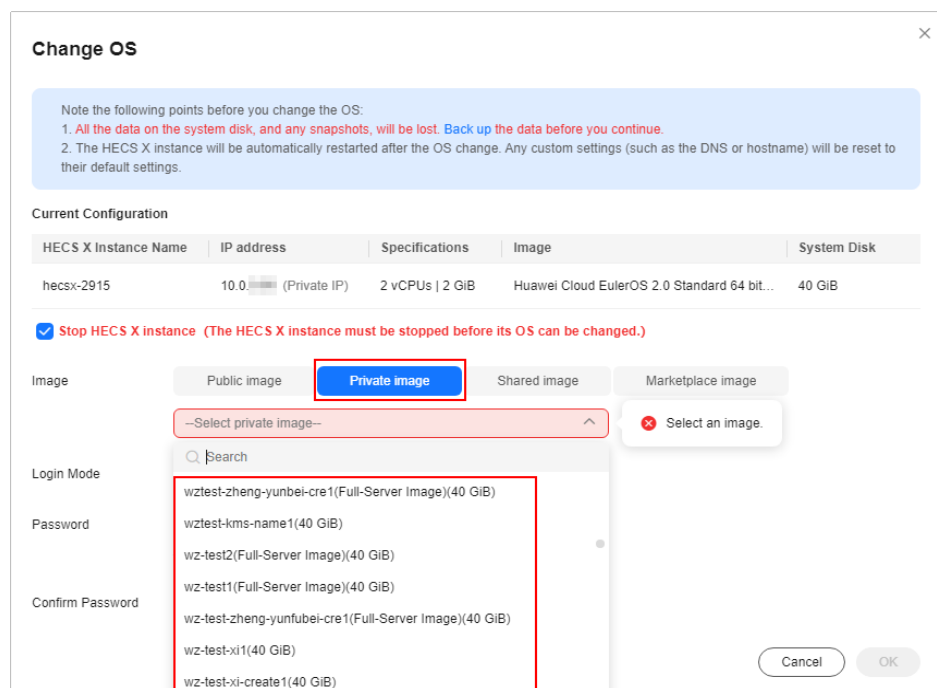
After creating or importing a private image using IMS, you can select the private image from the image list when creating a FlexusX instance. For details about how to purchase a FlexusX instance, see [Purchasing a FlexusX Instance](#).

Figure 4-1 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 4-2 Using a private image to change the OS of a FlexusX instance

4.3 Creating an Image from a FlexusX Instance

Scenarios

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

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

Constraints

- Only running or stopped FlexusX instances can be used to create private images.
- Do not restart, stop, reset the password of, or reinstall or change the OS of the selected FlexusX instance during image creation.


Billing

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

Procedure

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

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

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

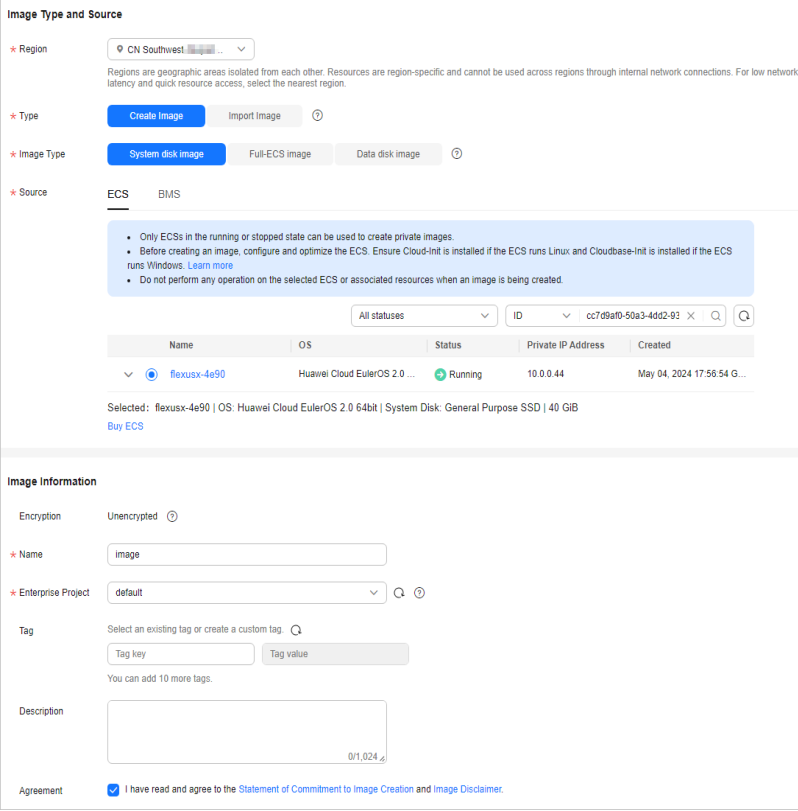


Image Type and Source

Region: CN Southwest



Type: **Create Image** | Import Image

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

Source: **ECS** | BMS

ECS

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

Name	OS	Status	Private IP Address	Created
 flexusx-4e90	Huawei Cloud EulerOS 2.0 ...	 Running	10.0.0.44	May 04, 2024 17:56:54 G...

Selected: flexusx-4e90 | OS: Huawei Cloud EulerOS 2.0 64bit | System Disk: General Purpose SSD | 40 GIB
[Buy ECS](#)

Image Information

Encryption: Unencrypted

Name: image

Enterprise Project: default

Tag:

Description:

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

Table 4-2 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 as required.
Source	<ul style="list-style-type: none">• If Image Type is set to System disk image or Full-ECS image, retain the default value.• If Image Type is set to Data disk image, select the data disk of the FlexusX instance you want to create an image from.

Table 4-3 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. <ul style="list-style-type: none">• 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.
Description	(Optional) Enter a description of the image.

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

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

 **NOTE**

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

Follow-Up Operations

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

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

4.4 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 optimal speed thanks to the optimization of the vCPU, memory, network, storage, kernel, application, and other settings. Typical applications, such as Nginx, Redis, and MySQL, can run 20% faster.

When you purchase a FlexusX instance, you need to select the Huawei Cloud EulerOS 2.0 image and then choose the application to be booted: Nginx, Redis, or MySQL. Then the Huawei Cloud EulerOS 2.0 image will pre-install the optimized version of Nginx, Redis, or MySQL to provide you with the optimal performance. For details about the performance benefits, see [Table 4-4](#).

Table 4-4 Performance improvement

Application	Default Version	Performance Improvement	Description
Nginx	1.21.5	<ul style="list-style-type: none">• 40% (small HTTP/HTTPS packets)• 15% (large packets)	The enhanced performance results from optimization at the application and OS layers.
MySQL	8.0.35	20% (OLTP read-only, write-only, and read/write)	
Redis	6.2.7	20% (small single-pipeline packets)	

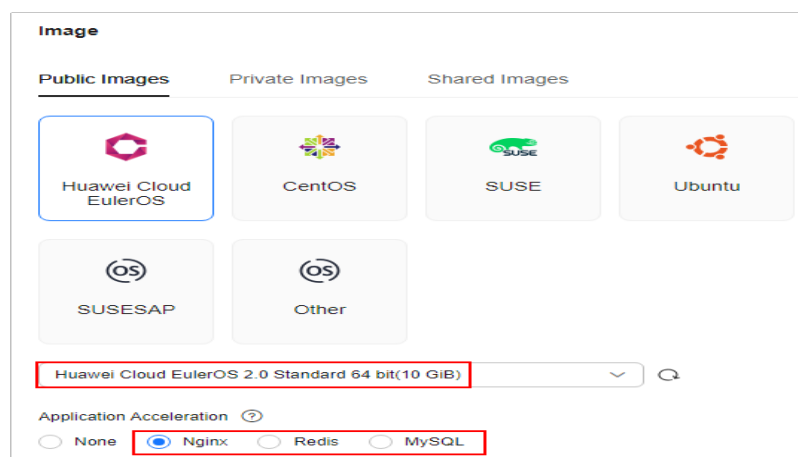
NOTE

- Based on the application acceleration type you configured, the default 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, or MySQL 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, or MySQL. For details about how to purchase a FlexusX instance, see [Purchasing a FlexusX Instance](#).

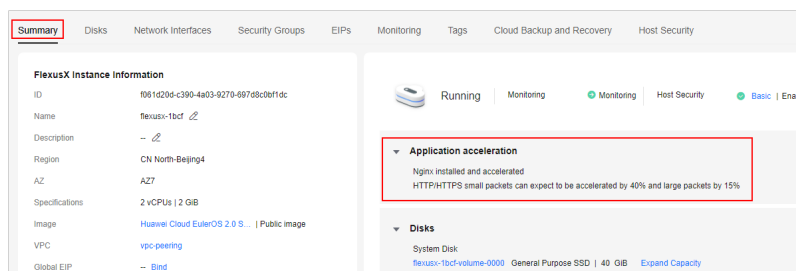
Figure 4-3 Enabling application acceleration



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 and project.
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, or MySQL 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

5 Managing EVS Disks

5.1 Overview

What Is EVS?

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.

Related Operations

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

Operation	Description
Detaching an EVS Disk	<ul style="list-style-type: none">• If 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 <ul style="list-style-type: none">• System disks do not need to be initialized.• Data disks containing data do not need to be initialized.

5.2 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 and project.
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.

Follow-Up Operations

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, see [Initializing an EVS Data Disk](#).

NOTE

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

5.3 Attaching Existing EVS Disks to a Flexus X 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 before EVS disks can be attached to it.
- A frozen EVS disk cannot be attached to a FlexusX instance.
- A SCSI EVS disk cannot be attached as the system disk to a FlexusX instance.
- A detached system disk can be used as a data disk for any FlexusX instances, but can only be used as a system disk for the FlexusX instance where it was attached before.
- A detached data disk that is purchased together with a FlexusX instance can only be used as a data disk for this instance.

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

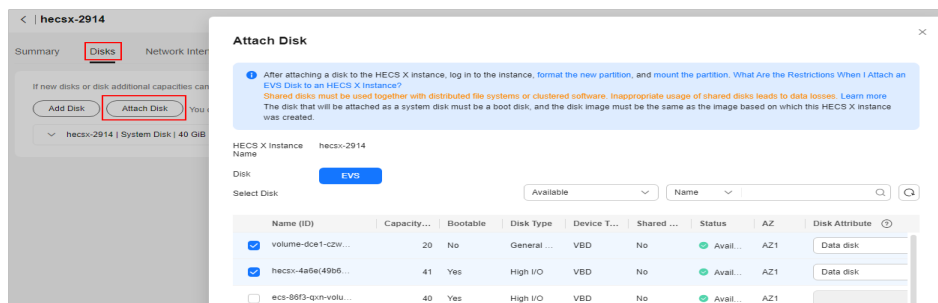
Prerequisites

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

Procedure

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

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

Figure 5-1 Attaching an EVS disk

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

Follow-Up Operations

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

5.4 Expanding the EVS Disk Capacity of a FlexusX Instance

Scenarios


If a disk on your FlexusX instance starts to run out of space, you can add capacity. Expanding the disk capacity does not affect the data on the disk.

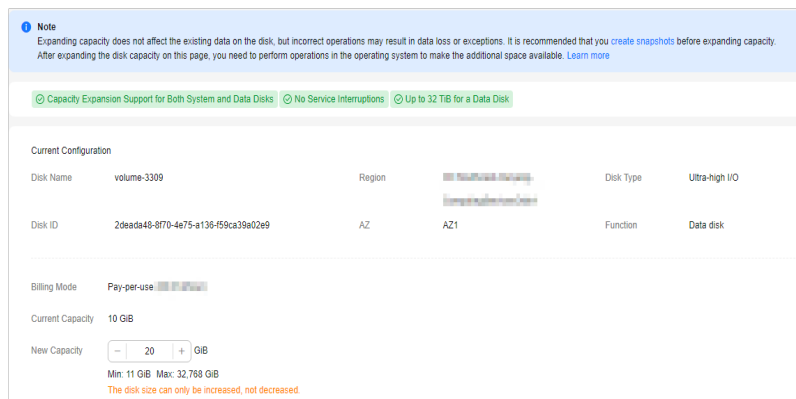
Billing

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 and project.
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.



Follow-Up Operations

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 uses 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.

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

5.5 Detaching an EVS Disk from a FlexusX Instance Online

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 re-attach the disk to the original FlexusX instance as the system disk.
- If you want to move a data disk from one FlexusX instance to another in the same region and AZ, you can detach the data disk and then attach it to that FlexusX instance.
- If you no longer need an EVS disk, you can detach and delete it.

Billing

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


Constraints

- A system disk can only be detached offline. 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.

Procedure

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

6 Managing Elastic Network Interfaces

6.1 Overview

Overview

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

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

Elastic Network Interface

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

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

Related Operations

Operation	Description
Attaching Extension Network Interfaces to a FlexusX Instance	If your FlexusX instance requires multiple network interfaces, you can attach extension network interfaces.

Operation	Description
Detaching Extension Network Interfaces from a FlexusX Instance	You can detach extension network interfaces from your FlexusX instance if they are no longer needed. Only extension network interfaces can be detached from the FlexusX instance. You cannot detach the primary network interface from it.
Changing the VPC for a FlexusX Instance	You can move your FlexusX instance from the current VPC to another.
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.

6.2 Attaching Extension Network Interfaces to a FlexusX Instance

Scenarios

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

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

Procedure


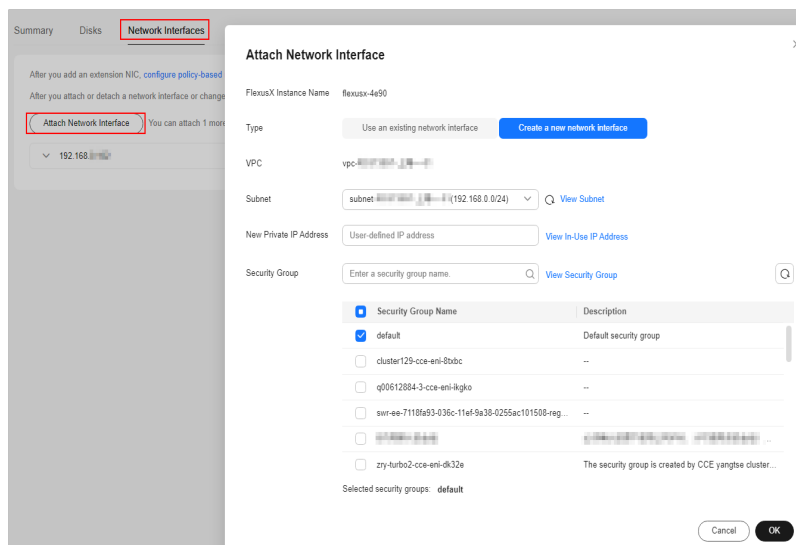
1. Log in to the FlexusX [console](#), in the upper left corner, click , and select a region and project.
2. In the FlexusX instance list, click the name of the FlexusX instance that you want to attach a network interface to.
The details page of this instance is displayed.
3. On the **Network Interfaces**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

Figure 6-1 Attaching an extension network interface

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

Related Operations

After an extension 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](#).


6.3 Detaching Extension Network Interfaces from a FlexusX Instance

Scenarios

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

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

Procedure

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

6.4 Changing the VPC for a FlexusX Instance

Scenarios

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

Constraints

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

Notes


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

NOTE

If you intend to change the VPC for a running FlexusX instance 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.

Procedure

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

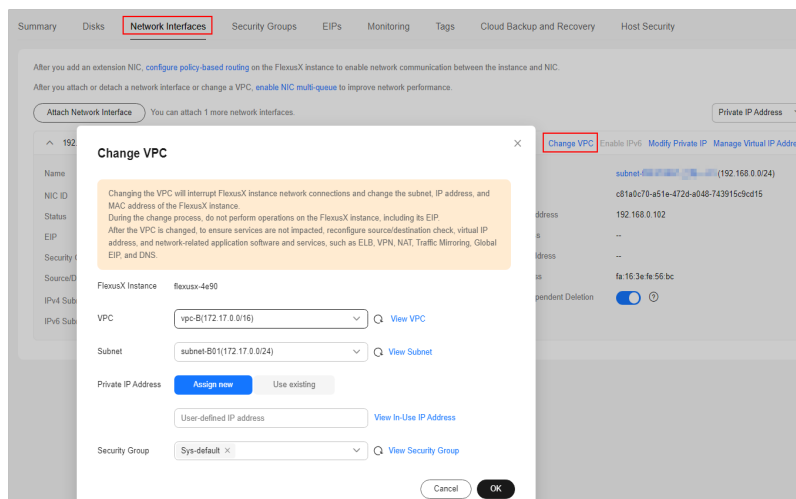
3. On the **Network Interfaces** tab, click **Change VPC**.

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 rules of all the selected security groups are applied to the FlexusX instance.

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 6-2 Changing a VPC

4. Click **OK**.

6.5 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.

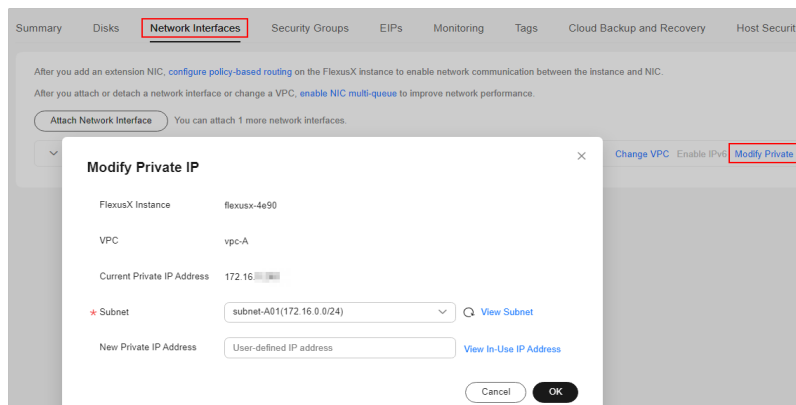
Constraints

- 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 and project.
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:** You can change the subnet when changing the private IP address.

NOTE

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

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


6.6 Configuring a Virtual IP Address for a FlexusX Instance

Scenarios

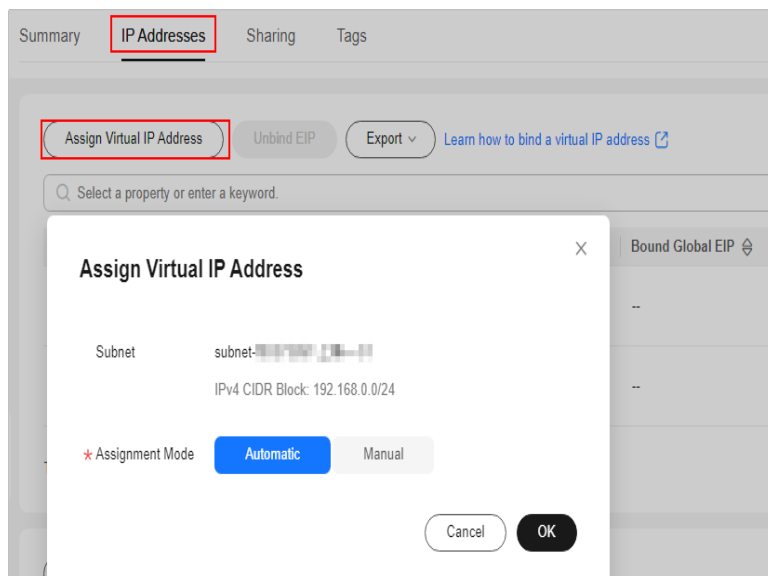
A virtual IP address serves as a secondary IP address for a network interface. A virtual IP address can be bound to multiple cloud servers to improve server availability.

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](#).

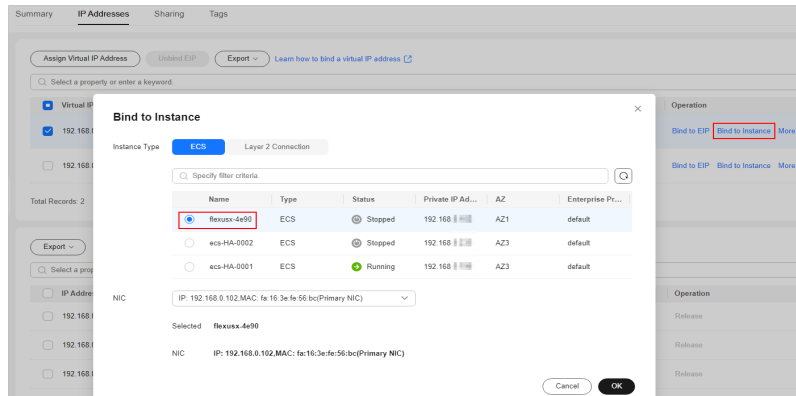
Procedure

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

7 Managing EIPs

7.1 Overview

What Is Elastic IP?

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

Related Operations

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


7.2 Binding an EIP to a FlexusX Instance

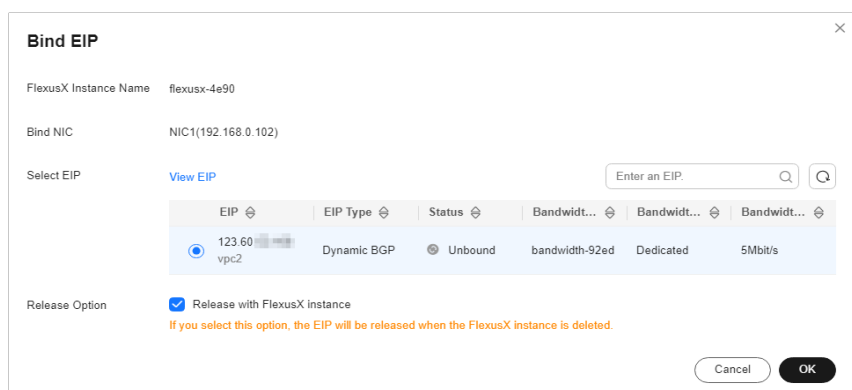
Scenarios

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

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

Procedure

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

7.3 Unbinding an EIP from a FlexusX Instance

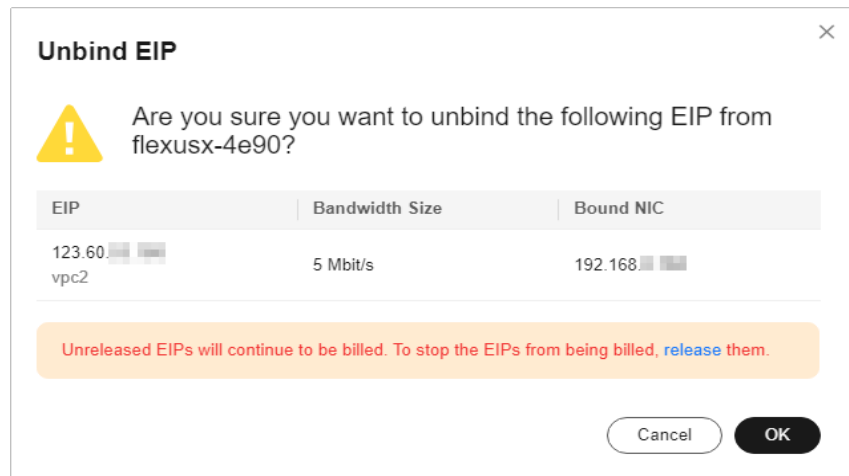
Scenarios

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

Procedure

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

2. Locate the target FlexusX instance, and in the **Operation** column, choose **More > Manage Network > Unbind EIP**.
3. Confirm the EIP information and click **OK**.



NOTE

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

7.4 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 modify the name, billing mode, and size of a bandwidth. This section describes how to modify the bandwidth of a FlexusX instance.

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

Table 7-1 Rules for modifying the bandwidth of EIPs in different billing modes

EIP Billing Mode	Billing Mode Changeable	Bandwidth Change	Billing Description
Yearly/ Monthly	No	<ul style="list-style-type: none"> • You can increase the bandwidth. The change is applied immediately. • You can decrease the bandwidth, but you need to renew the EIP, and the decreased bandwidth will 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. 	<ul style="list-style-type: none"> • Increasing bandwidth The increased bandwidth will be billed accordingly. • Decreasing bandwidth The new bandwidth will be billed when the new subscription period starts.
Pay-per-use	Yes	You can increase or decrease the bandwidth. The changes are applied immediately.	Pay-per-use billing is a postpaid mode, so after the bandwidth is modified, you will be billed based on the new billing mode.

NOTE


- The yearly/monthly and pay-per-use billing modes in [Table 1](#) define how an EIP is billed, not how the FlexusX instance is billed.
Yearly/Monthly EIPs can only be billed by bandwidth, 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.

The screenshot shows the 'EIP' configuration page. Under the 'Billed By' section, three options are available: 'Bandwidth' (For heavy/stable traffic), 'Traffic' (For light/sharply fluctuating traffic), and 'Shared bandwidth' (For staggered peak hours). The 'Traffic' option is highlighted with a red box. Below the options, a note states: 'Billed based on total traffic irrespective of usage duration; configurable maximum bandwidth size.'

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 modified. A yearly/monthly EIP can only be billed by bandwidth.
 - The bandwidth size can be increased in the current subscription period, and decreased for the renewal period.
- Only the bandwidths of pay-per-use EIPs billed by bandwidth or traffic can be modified in batches. The bandwidths of yearly/monthly EIPs or pay-per-use EIPs billed by shared bandwidth cannot be modified in batches.

Procedure

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

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

8 Managing Server Security

8.1 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 8-1 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.	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• Enhancing the Login Password Strength• Improving the Port Security• Periodically Upgrading the OS

Enabling HSS

HSS is designed to improve the overall security for cloud servers. It helps you identify and manage the assets on your servers, eliminate risks, and defend

against intrusions and web page tampering. There are also advanced protection and security operations functions available to help you easily detect and handle threats.

- You can enable HSS (basic edition) when purchasing a 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 key to ensuring FlexusX instance reliability, availability, and performance. Using monitoring data, you can determine 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 [Managing Server 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 consistency of your data.

- You can enable CBR when purchasing a Flexus X 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 8-2 lists some high-risk ports. Do not use these ports for your services.

Table 8-2 High-risk ports

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

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](#).

8.2 Configuring the Security Group for a FlexusX Instance

8.2.1 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.

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

NOTE

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

Security Group Rules

After a security group is created, you can add rules to 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 create a custom security group or use the default one provided by the system. The default security group permits all outbound traffic and denies inbound traffic. FlexusX instances in a security group can communicate with each other.

Table 8-3 Default security group rules

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

Security Group Constraints

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


8.2.2 Configuring Security Group Rules for a FlexusX Instance

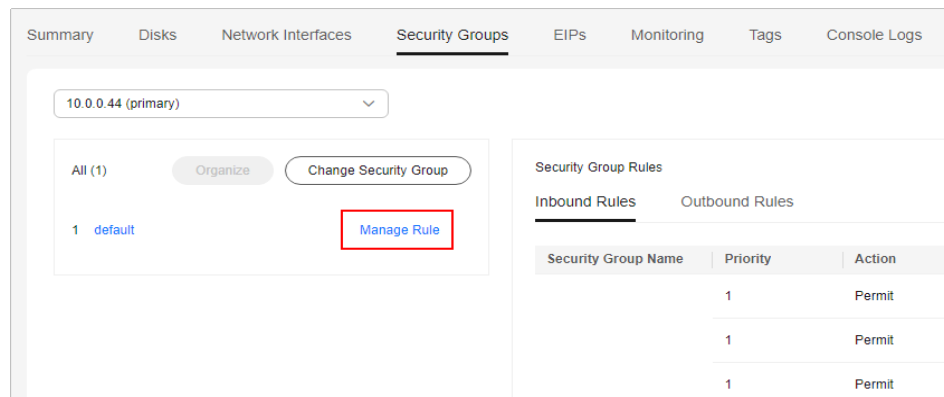
Scenarios

Similar to 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.

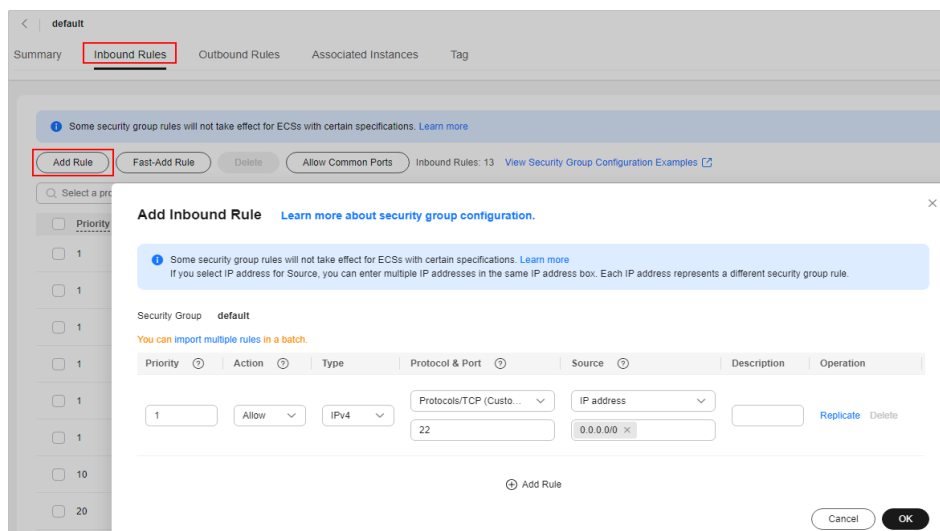
- Inbound rules allow or deny incoming network traffic to FlexusX instances in the security group.
- Outbound rules allow or deny outgoing network traffic from FlexusX instances in the security group.

Procedure

1. Log in to the FlexusX [console](#), in the upper left corner, click , and select a region and project.
2. On the **FlexusX Instances** page, locate the FlexusX instance and click its name.
The details page of this instance is displayed.
3. On the detailed page, click the **Security Groups** tab and view security group rules.
4. Click **Manage Rule**.
The page for configuring security group rules is displayed.



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

Figure 8-1 Adding an inbound rule

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

Verifying Security Group Rules

After adding inbound and outbound rules, you can verify whether the rules have been applied. Assume that you have deployed a website on a FlexusX instance. To enable users to access your website through HTTP (80), you need to add an inbound rule to the security group of the FlexusX instance to allow access over this port. [Table 8-4](#) shows the rule details.

Table 8-4 The security group rule

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

Linux

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

1. Log in to the FlexusX instance.
2. Check whether TCP port 80 is listened on:

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

If command output shown in [Figure 8-2](#) is displayed, TCP port 80 is listened on.

Figure 8-2 Command output for the Linux FlexusX instance

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

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

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

Impacts of Deleting Common Security Group Rules

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

Deleting security group rules will disable some functions.

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

8.2.3 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


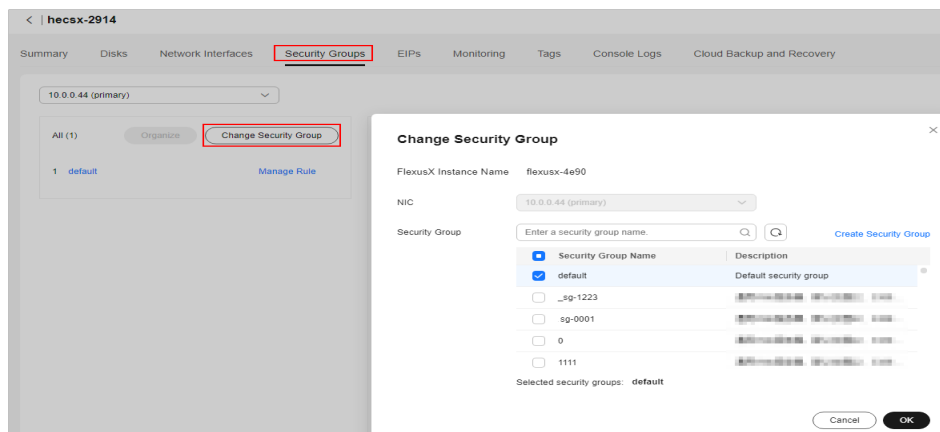
1. Log in to the FlexusX [console](#), in the upper left corner, click  , and select a region and project.
2. On the **FlexusX Instances** page, locate the FlexusX instance and click its name.
The details page of this instance is displayed.
3. On the **Security Groups** tab, click **Change Security Group**.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

Figure 8-3 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**.

8.3 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.

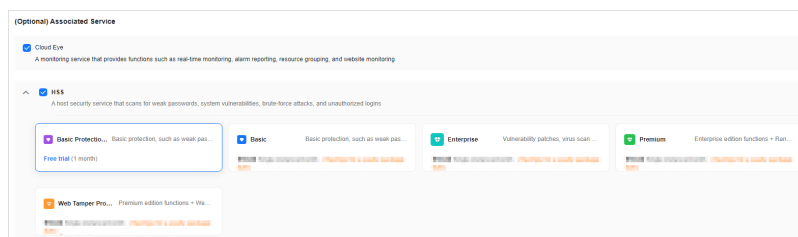
For more information about HSS, see [What Is HSS?](#)

Enabling HSS

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

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

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

Figure 8-4 Enabling HSS when purchasing a FlexusX instance

Select one of the following options:

- **Basic edition (one-month free trial):** After this function is enabled, the HSS basic edition can be used free of charge for 30 days. The HSS basic edition supports detection of OS vulnerabilities, weak passwords, and brute force cracking to improve the overall security for your ECSs.

NOTE

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

If you want to retain or upgrade HSS security capabilities, you are advised to enable the advanced HSS edition. For details, see [What Should I Do When the Free Trial of HSS Basic Edition Expires?](#)

This option is selected by default.

- **Advanced HSS edition (paid):** You can choose from HSS basic, enterprise, premium, and Web Temper Protection (WTP) editions and you need to pay for it.

After ECSs are purchased, you can switch between different editions on the HSS console after **Advanced HSS edition (paid)** is enabled. For details about the differences among different editions, see [Specifications of Different Editions](#).

- **None:** HSS is disabled and servers are not protected.

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

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

NOTE

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


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

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

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

Viewing the Security Status of FlexusX Instances

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

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

9 Managing Backups

9.1 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 consistency of your data.

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

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

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

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

Related Operations

Operation	Description
Associating a FlexusX Instance with a Backup Vault	If you want to back up a FlexusX instance, associate the instance with a backup vault first.
Backing Up a FlexusX Instance	CBR enhances data integrity and service continuity. After a FlexusX instance is backed up, if anything should happen 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 .

9.2 Associating a FlexusX Instance with 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.


Constraints

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

Billing

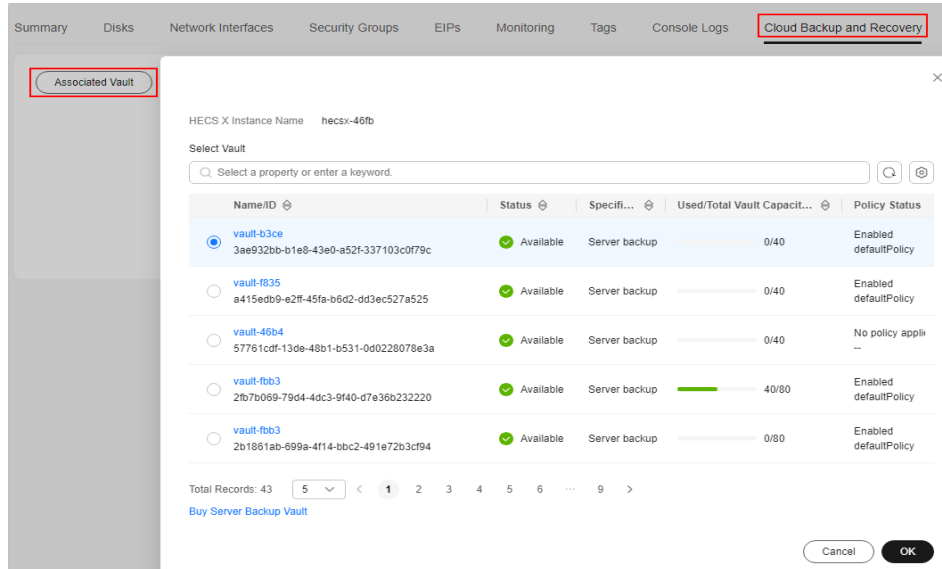
See [CBR Billing Overview](#).

Procedure

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

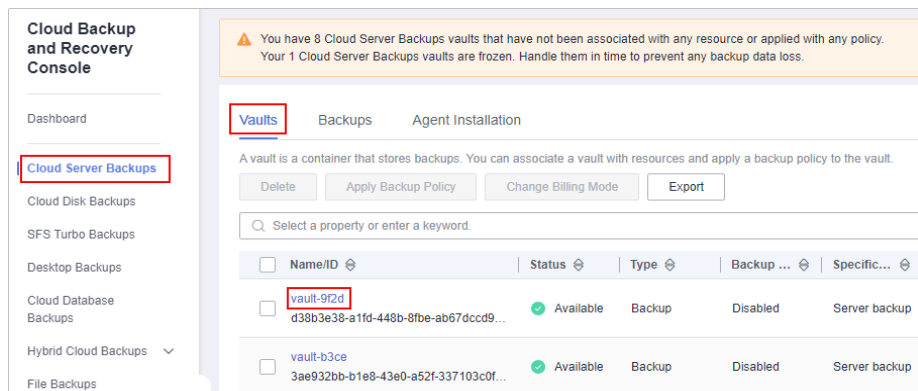
- You can click **Create Server Backup** to purchase a server backup vault on the CBR console. For details, see [Purchasing a Server Backup Vault](#).
- You can click **Create Disk Backup** to purchase a disk backup vault on the CBR console. For details, see [Purchasing a Disk Backup Vault](#).

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



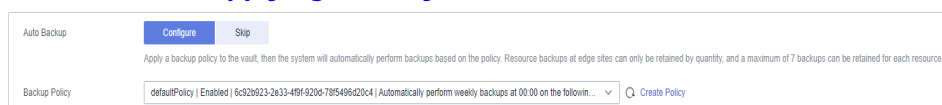
3. View the backup vaults.

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



Follow-Up Operations

- 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](#).

9.3 Backing Up a FlexusX Instance

Scenarios

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

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


Prerequisites

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

Constraints


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

Procedure

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

NOTE

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

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

- To create a cloud disk backup:

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

- In the disk list, all disks are selected by default. You can select the disks to be backed up.
 - **Name:** Customize your backup name.
 - **Description:** Enter the supplementary information about the backup.
 - **Full Backup:** If this option is selected, the system will perform full backup for the disks selected. The storage capacity used by the backup increases accordingly.
3. Click **OK**. The system creates a backup immediately.
 4. Click **Go to Backup List**.

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

Follow-Up Operations

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

10 Managing Server Monitoring

10.1 Overview

What Is Server Monitoring?

Monitoring is key for ensuring FlexusX instance performance, reliability, and availability. Using monitoring data, you can determine how well your FlexusX instance resources are being used. You can use Cloud Eye to track the statuses of your cloud servers. Cloud Eye automatically monitor cloud servers in real time and makes it easier to manage alarms and notifications, so that you can track cloud server performance metrics.

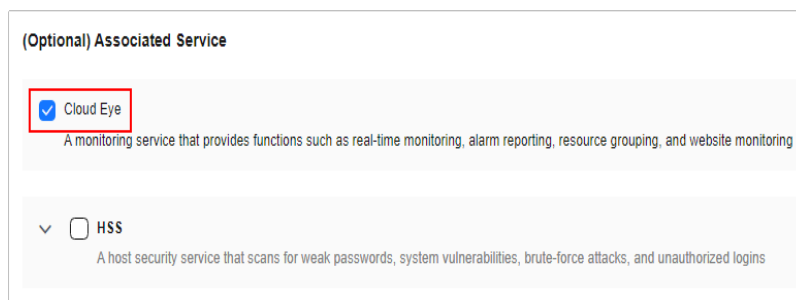
Server monitoring consists of basic monitoring, OS monitoring, and process monitoring.

- 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.

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 the 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 10-1 Selecting Cloud Eye

- If you do not select Cloud Eye, you will only have 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.

Related Operations

Operation	Description
Configuring Alarm Rules for a FlexusX Instance	After monitoring is enabled, you can configure alarm rules to ensure you 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.

Helpful Links

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


10.2 Configuring Alarm Rules for a FlexusX Instance

Scenarios

Configuring alarm rules for FlexusX instances allows you to customize the monitored objects and notification policies. They let 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](#).
2. Click  in the upper left corner and select the desired region and project.
3. In the navigation pane, choose **Alarm Management > Alarm Rules**.
4. On the **Alarm Rules** page, click **Create Alarm Rule** to create one, or modify an existing alarm rule.
 - [Creating an Alarm Rule](#)
 - [Modifying an Alarm Rule](#)

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

NOTE

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

10.3 Viewing Monitoring Metrics of a FlexusX Instance

Scenarios

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

Prerequisites


- The FlexusX instance is running properly.

Cloud Eye does not display the monitoring data for a stopped, faulty, or deleted FlexusX instance. After such a FlexusX instance restarts or recovers, the monitoring data is available on Cloud Eye.
- ### NOTE
- Cloud Eye discontinues monitoring FlexusX instances that remain in the **Stopped** or **Faulty** state for 24 hours and removes them from the monitoring list. However, the alarm rules configured for such FlexusX instances are not automatically deleted.
- Alarm rules have been configured on Cloud Eye for the 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 and project.
2. Click the name of the target FlexusX instance.

3. Click the **Monitoring** tab to view the monitoring data.

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

It takes a bit of time to transmit and display the monitoring data. There is about a 5- to 10- minute delay before the monitoring data can be displayed, so it takes about that long before the monitoring data of a newly created FlexusX instance shows up.