Intelligent Edge Cloud

User Guide

Issue	12
Date	2022-04-07



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2022. 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 Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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.

Contents

1 IEC Console Overview....1
2 Creating an IAM User and Granting IEC Permissions....5
3 Edge Services....7
3.1 Edge Service Overview....7
3.2 Creating an Edge Service....8
3.3 Viewing Edge Service Information....17
3.4 Expanding an Edge Service....18
3.5 Deleting an Edge Service....18
3.6 Examples of Edge Instance Distribution....19
4 Edge Instances....21
4.1 Edge Instance Overview....21
4.2 Edge Instance Lifecycle....22
4.3 Edge Instance Types....23
4.4 Viewing Edge Instance Information....24
4.5 Logging In to an Edge Instance....26
4.6 Managing an Edge Instance....28
4.7 Changing the Edge Instance OS....30
4.8 Creating a Key Pair....32
5 Edge Images....39
5.1 Edge Image Overview....39
5.2 Using IMS to Create an IEC Private Image....40
5.3 Using an Edge Instance to Create an IEC Private Image....41
5.4 Viewing Edge Image Information....43
5.5 Deleting an IEC Private Image....44
6 Edge Networks....45
6.1 Edge Network Overview....45
6.2 VPCs....50
6.2.1 Creating a VPC....50
6.2.2 Managing VPCs....51
6.2.3 Managing Subnets....52
6.3 Route Tables....53

 Copyright © Huawei Technologies Co., Ltd.

6.3.1 Creating a Route Table ... 53
6.3.2 Managing Custom Route Tables ... 55
6.3.3 Adding a Route ... 55
6.3.4 Managing Custom Routes ... 57
6.3.5 Associating a Subnet with a Custom Route Table ... 57
6.3.6 Disassociating a Subnet from a Custom Route Table ... 58
6.3.7 Changing the Custom Route Table Associated with a Subnet ... 59
6.4 Bandwidths ... 59
6.4.1 Viewing Bandwidth Information ... 59
6.4.2 Modifying a Bandwidth ... 61
6.4.3 Deleting a Bandwidth ... 62
6.5 EIPs ... 62
6.5.1 Assigning an EIP and Binding It to an Edge Instance or Virtual IP Address ... 63
6.5.2 Viewing EIP Information ... 63
6.5.3 Unbinding or Releasing an EIP ... 64
6.6 Virtual IP Addresses ... 65
6.6.1 Assigning a Virtual IP Address ... 65
6.6.2 Managing Virtual IP Addresses ... 65
6.6.3 Binding a Virtual IP Address to an EIP or Edge Instance ... 66
6.7 Security Groups ... 68
6.7.1 Creating a Security Group ... 68
6.7.2 Managing a Security Group ... 69
6.7.3 Configuring Security Group Rules ... 70
6.7.4 Managing Security Group Rules ... 73
6.7.5 Importing or Exporting Security Group Rules ... 74
6.7.6 Changing a Security Group ... 75
6.7.7 Security Group Configuration Examples ... 76
6.7.8 Commonly Used Ports ... 79
6.8 Network ACLs ... 80
6.8.1 Creating a Network ACL ... 80
6.8.2 Managing Network ACLs ... 81
6.8.3 Configuring a Network ACL ... 82
6.8.4 Managing Network ACL Rules ... 85
6.8.5 Importing or Exporting Network ACL Rules ... 86
6.8.6 Network ACL Configuration Examples ... 87
6.8.7 Associating a Network ACL with Subnets ... 89
6.8.8 Disassociating a Network ACL from a Subnet ... 90
6.8.9 Changing the Priority of a Network ACL Rule ... 90

7 Monitoring ... 92

7.1 Viewing Edge Instance Monitoring Data ... 92
7.2 Metrics ... 93
7.3 Viewing Bandwidth and EIP Monitoring Data ... 95

 Copyright © Huawei Technologies Co., Ltd.

7.4 Bandwidth and EIP Metrics 97

8 Alarm 99

8.1 Creating an Alarm Rule 99
8.2 Managing Alarm Rules 101
8.3 Configuring an Alarm Notification 103
8.4 Managing Alarm Notifications 105
8.5 Viewing the Alarm History 106

9 Quota Adjustment 108

10 Common Operations 110

10.1 Deleting Files in the Network Rule Directory 110
10.2 Detaching Data Disks from an Edge Instance 111
10.3 Troubleshooting the Issue that a Key Pair Created Using **puttygen.exe** Cannot Be Imported to the Management Console 113
10.4 Configuring Policy-based Routing for an Edge Instance with Multiple NICs 115
10.5 Accessing the Internet Using an EIP Bound to an Extension NIC 119

A Change History 121

 Copyright © Huawei Technologies Co., Ltd.

1 IEC Console Overview

Table 1-1 lists the function provided by the IEC console.

Table 1-1 IEC functions

Category	Function Description	Helpful Link
Permissions	With Identity and Access Management (IAM), you can use your HUAWEI CLOUD account to create IAM users, and assign access permissions to these users for specific resources.	Creating an IAM User and Granting IEC Permissions
Edge services	An edge service is a logical collection of a variable quantity of compute instances, including instance specifications, images, disks, and networks, coupled with their scheduling policies and distribution. You specify the quantity, scheduling policies, and distribution of edge instances to create an edge service.	Creating an Edge Service
		Deleting an Edge Service
		Expanding an Edge Service
Edge instances	An edge instance is a cloud server dedicated to edge use. It includes vCPU, memory, OS, and disks. IEC automatically creates an edge instance after you create an edge service. You can start, stop, restart, or delete an edge instance, or change the edge instance OS and name.	Managing an Edge Instance
Edge images	An image is an instance template that contains an OS or service data and may also contain private software and application software, such as database software. IEC supports both public images and private images for the edge.	Using IMS to Create an IEC Private Image
		Using an Edge Instance to Create an IEC Private Image

Copyright © Huawei Technologies Co., Ltd.

Category	Function Description	Helpful Link
		Deleting an IEC Private Image
VPCs	A Virtual Private Cloud (VPC) provides an isolated virtual network for your cloud resources. You can configure and manage the networks in the VPC, making changes to these networks quickly and securely. Each VPC consists of a private CIDR block and at least one subnet. IEC allows you to create VPCs and subnets and delete them if they are no longer needed.	**Creating a VPC**
		Deleting a VPC
		Deleting a Subnet
Routes and **route tables**	A route is configured with the destination, next hop type, and next hop to determine where the network traffic is directed. A route table contains a set of rules, called routes, that are used to control where inbound and outbound subnet traffic is forwarded within a VPC. IEC allows you to create route tables, add routes to a route table, associate a subnet with a custom route table, and change the custom route table associated with a subnet.	**Creating a Route Table**
		Adding a Route
		Associating a Subnet with a Custom Route Table
		Changing the Custom Route Table Associated with a Subnet
Bandwidths	IEC provides edge site-level bandwidth sharing and multiplexing capabilities. All EIPs using the same carrier line share the same bandwidth. Different carrier lines use different bandwidths. If you assign an EIP for the first time and the carrier line using the EIP does not have a shared bandwidth allocated to it, the system automatically allocates a shared bandwidth to the carrier line. Different lines use different bandwidths.	**Modifying a Bandwidth**
		Deleting a Bandwidth
EIPs	An EIP is a public IP address that is used to access the Internet. You can bind an EIP to or unbind an EIP from an edge instance or a virtual IP address.	**Assigning an EIP and Binding It to an Edge Instance or Virtual IP Address**
		Assigning an EIP and Binding It to an Edge Instance or Virtual IP Address
		Unbinding or Releasing an EIP

Copyright © Huawei Technologies Co., Ltd.

Category	Function Description	Helpful Link
		Releasing an EIP
Virtual IP addresses	A virtual IP address is an IP address that is not allocated to an edge instance NIC. You can access an edge instance through a virtual IP address. IEC allows you to assign and delete virtual IP addresses, and bind a virtual IP address to an EIP or edge instance.	Assigning a Virtual IP Address
		Deleting a Virtual IP Address
		Binding a Virtual IP Address to an EIP or Edge Instance
Security groups	A security group is a collection of access control rules for edge instances that have the same security protection requirements and are mutually trusted within a VPC. After you create a security group, you can create different inbound and outbound rules for the security group. These rules will apply to any edge instance that you add to this security group. You can create, change, or delete security groups, configure inbound and outbound rules for each security group, and import or export security group rules.	Creating a Security Group
		Changing a Security Group
		Deleting a Security Group
		Configuring Security Group Rules
		Importing or Exporting Security Group Rules
Network ACLs	A network access control list (ACL) is an optional security layer for your subnets. You associate one or more subnets with a network ACL. The network ACL can help control traffic in and out of the subnets. Similar to security groups, network ACLs control access to the network. They add an additional layer of defense to your VPC. You can create and manage network ACLs, configure inbound and outbound rules for each network ACL, import or export network ACL rules, and associate a subnet with a network ACL.	Creating a Network ACL
		Managing Network ACLs
		Configuring a Network ACL
		Configuring a Network ACL
		Importing or Exporting Network ACL Rules
		Associating a Network ACL with Subnets
		Disassociating a Network ACL from a Subnet
		Changing the Priority of a Network ACL Rule

Copyright © Huawei Technologies Co., Ltd.

Category	Function Description	Helpful Link
Server monitoring	Server monitoring enables you to view the performance metrics and running status of your edge instances.	**Viewing Edge Instance Monitoring Data**
		Metrics
Bandwidth and EIP metrics	Bandwidth monitoring helps you learn about the metrics of and alarms generated for EIPs and bandwidths.	**Viewing Bandwidth and EIP Monitoring Data**
		Bandwidth and EIP Metrics
Alarms	You can set alarm rules for monitoring metrics. When the monitoring metrics trigger the preset alarm conditions, IEC notifies you by email or SMS message. In this way, you can handle faults in a timely manner to prevent business loss caused by resource problems. IEC allows you to create alarm rules, configure alarm notifications, and view historical alarms.	**Creating an Alarm Rule**
		Configuring an Alarm Notification
		Viewing Historical Alarms
Quotas	Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas limit the number or amount of resources available to users, for example, the maximum number of edge services and edge instances you can create. You can also increase the quota if the existing quota cannot meet your service requirements.	**Quota Adjustment**

Copyright © Huawei Technologies Co., Ltd.

2 Creating an IAM User and Granting IEC Permissions

Scenarios

If you need to assign different permissions to allow users access to your IEC resources, use IAM to manage fine-grained permissions. IAM provides identity authentication, permissions management, and access control, securing access to your HUAWEI CLOUD resources.

With IAM, you can use your HUAWEI CLOUD account to create IAM users and assign permissions to these users to control their access to specific resources.

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing IEC resources.
- Grant only the permissions required for users to perform specific tasks.

Skip this section if your HUAWEI CLOUD account does not need individual IAM users.

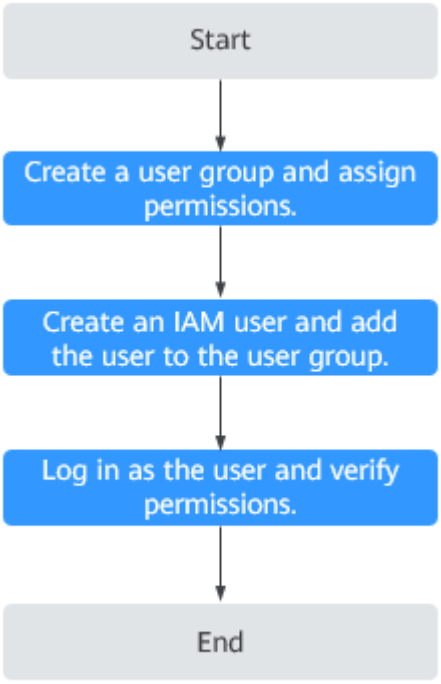
IAM is free. You pay only for resources purchased using your account. For more information about IAM, see **IAM Service Overview**.

For more information about IEC permissions, see **Permissions Management**.

Copyright © Huawei Technologies Co., Ltd.

Process Flow

Figure 2-1 Granting IEC permissions



1. **Create a user group and assign permissions** to it.

   Create a user group on the IAM console, and assign the **IEC ReadOnlyAccess** policy to the group.

2. **Create an IAM user**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the IEC console with the credentials of the user created in the previous step and verify that the user only has read permissions for IEC resources.

   Choose **Service List** > **Intelligent Edge** > **Intelligent EdgeCloud**. If the user can view the edge service list but cannot create edge services, the IEC ReadOnlyAccess policy has taken effect.

Copyright © Huawei Technologies Co., Ltd.

3 Edge Services

3.1 Edge Service Overview

IEC allows you to create edge services to facilitate resource management across **IEC sites**.

An edge service is a logical collection of a variable quantity of compute instances, including instance specifications, images, disks, and networks, coupled with their scheduling policies and distribution.

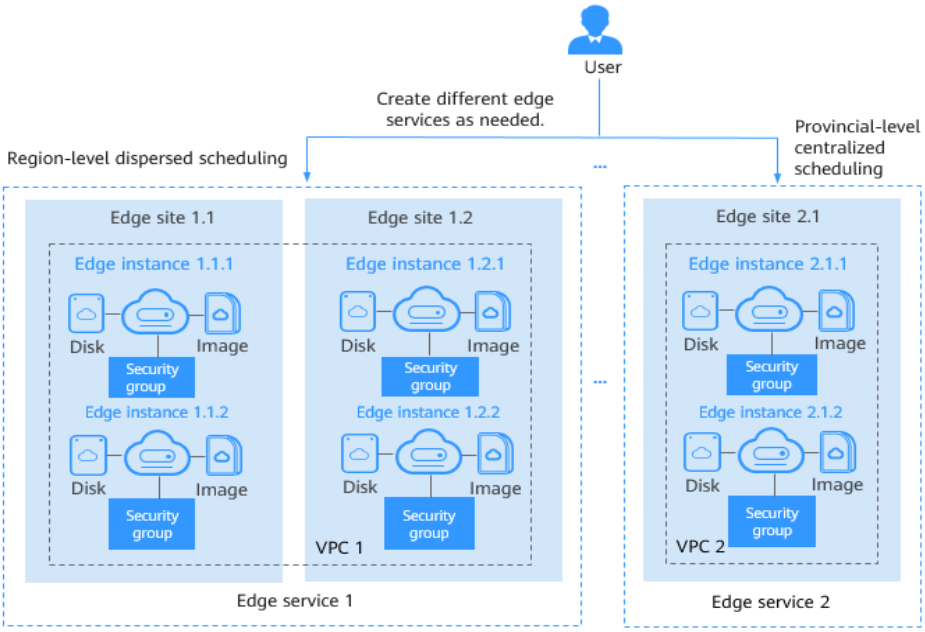
Based on different resource management needs, such as different instance specifications and scheduling policies, you can create multiple different edge services.

Figure 3-1 shows two different edge services.

- **Edge service 1**: Workloads are distributed across the region. Two instances are deployed at edge sites 1.1 and 1.2, respectively. (The four instances have the same resource configurations.)
- **Edge service 2**: Workloads are distributed across the province. Two instances with the same configurations are deployed at edge site 2.1.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-1 Edge service



After you create an edge service, you can view its basic information, and the quantity and distribution of edge instances it contains. You can also expand the edge service capacity by adding more instances.

3.2 Creating an Edge Service

Scenarios

After you **make all preparations**, you can create **edge services** based on your requirements.

The following is the procedure of creating an edge service on the IEC console. For details about how to use IEC APIs, see the *Intelligent EdgeCloud API Reference*.

Prerequisites

- You have registered with HUAWEI CLOUD, completed real-name authentication, and topped up your account. Your application for the permissions on provisioning IEC resources has been approved. For details, see **Make Preparations**.
- You have **created a VPC**. For more information about the edge network, see **Edge Network Overview**.
- You have **created a security group** and **configured security group rules**. For more information, see **Edge Network**.
  - To allow the edge instance to be pinged, **add an inbound security group rule to allow the ICMP protocol**.

 Copyright © Huawei Technologies Co., Ltd.

  - To allow remote login to a Linux edge instance through SSH, **allow access to port 22 in the inbound direction of the security group**.
- You have created an IEC private image (if required). For details, see **Edge Images**.

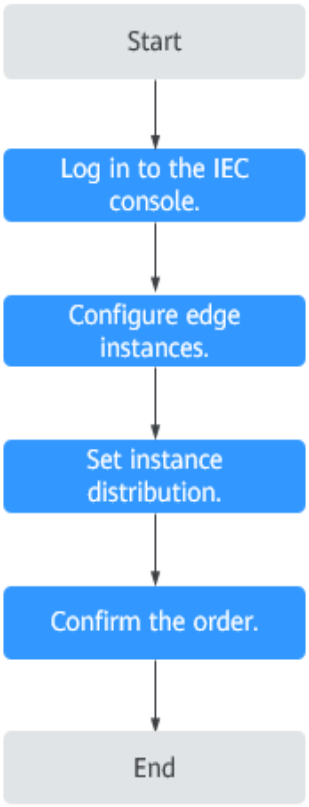
Constraints and Limitations

- By default, you can use one HUAWEI CLOUD account to create a maximum of 10 edge services. If you want to create more edge services, increase the quota by referring to **Quota Adjustment**.
- By default, you can use one HUAWEI CLOUD account to create a maximum of 50 edge instances. If you want to create more edge instances, increase the quota by referring to **Quota Adjustment**. You can create a maximum of 10 instances at a single location at a time. If you need to create more instances at this location, expand the edge service after it is created.
- By default, you can use one HUAWEI CLOUD account to create instances at a maximum of 10 locations when creating an edge service. If you need to create instances at more locations for the same edge service, you can expand the edge service to add more instances at these locations after the edge service is created.

Procedure

Figure 3-2 shows the process of creating an edge service.

Figure 3-2 Creating an edge service



Copyright © Huawei Technologies Co., Ltd.

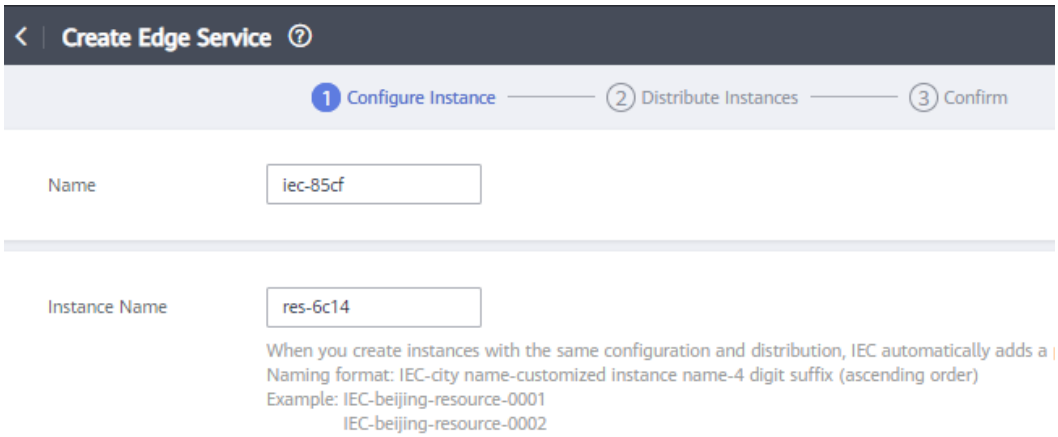
Step 1 Log In to the IEC Console

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

Step 3 On the displayed IEC console, click **Create Edge Service**.

The **Create Edge Service** page is displayed.



----End

Step 2 Configure Edge Instances

Set the parameters based on **Table 3-1** and click **Next: Distribute Instances**.

Table 3-1 Parameter description

Parameter	Description	Example Value
Name	Enter a name that is easy to identify for the edge service. The name can contain 1 to 32 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.	Live transcoding_Suzhou

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Instance Name	Enter a name that is easy to identify. • The name can contain 1 to 48 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed. • If you create more than one edge instance in an edge service, the system will automatically add a prefix and a suffix to the instance name to differentiate instances. Naming format: IEC-*[city abbreviation]-[name]-xxxx* (ascending order) Example: **IEC-BJ-resource-0001**, **IEC-BJ-resource-0002**, and **IEC-BJ-resource-0003** Policy for processing special characters in city names (city names indicates instance locations): – Spaces will be deleted. For example, **wu han** is changed to **wuhan**. – Apostrophes (') or backticks (`) will be replaced by underscores (_). For example, **xi'an** is changed to **xi_an**. – Phonetic symbols will be deleted. For example, **ürümqi** is changed to **urumqi**. **NOTE** • If the city name has an abbreviation, the abbreviation will be used preferentially. If the city name does not have an abbreviation, the first four letters of the city name will be used. • If there is more than one edge site in a city, the system will add serial numbers to the city name in the format of *[city abbreviation]* + *[serial number]*, for example, **BJ01**.	resource
Instance Name Prefix	This option is enabled by default. If you disable this option, instances will be named in the format of *[name]-xxxx* (ascending order), and the instance name can contain a maximum of 59 characters.	N/A

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Specifications	Select the edge instance type and specifications. • General computing (S6) • Memory-optimized (M6) • General computing-plus (C6 and C6s) • AI-accelerated (AI1) • GPU-accelerated (G5r and PI2) • Disk-intensive (D3i)	AI-accelerated | ai1.xlarge.4 | 4 vCPUs | 16 GiB
Image Type/ Image	Select a public or private image that you want to use to create edge instances. For image details, see **Edge Image Overview**.	Public image Public-ai1-Standard
System Disk/ Data Disk	By default, **High I/O** is selected. Select a disk type and set the disk capacity based on service requirements.	System Disk: High I/O, 100 GB Data Disk: High I/O, 120 GB
Edge VPC	Select the VPC where the edge instances will reside. If no VPCs are available, click **Create a VPC**.	vpc-001(172.16.0.0/16)
Extension NIC	Specify whether to bind extension NICs to edge instances. If you select **None**, the system will create only the primary NIC. If you specify the quantity of extension NICs, go to the edge instance details page to **add a NIC** after you create the edge service.	1
Bind EIP	Specify whether you want to bind an EIP to each edge instance. • If you enable this option, IEC will automatically bind an EIP to each edge instance. • If you disable this option, manually assign an EIP and bind it to the edge instance after you create the edge service. For details, see **Assigning an EIP**. If you do not bind an EIP to an edge instance, the edge instance can access the Internet.	Enable
Security Group	Select one or more security groups for the edge instances. If no option is available, **create a security group** and **configure security rules**.	Security_Group_001

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Login Mode	You can **log in to an edge instance** using any of the following methods: • **Password**: A username and its initial password will be used for edge instance authentication. If edge instances run Linux, use username **root** and its initial password to log in. If edge instances run Windows, use username **Administrator** and its initial password to log in. **Password** can be used for both public and private images. Passwords must meet the following complexity requirements: – Must contain 8 to 26 characters. – Must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters !@$%^-_=+[{}]:,./? – Cannot contain the username or the username backwards. • **Key pair**: A key pair will be used for edge instance authentication. You can select an existing key pair or **create a key pair**. **Key pair** is recommended because it is more secure than **Password**. If you select **Password**, ensure that the password meets complexity requirements to prevent malicious attacks. If you use an existing key pair, make sure that you have saved the key file locally. Otherwise, you will not be able to log in to the edge instance. • **Inherit password from image**: The password of the selected image will be used for login. This method is used only for private images. To use this method, ensure that you have set a password for the image.	N/A

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Advanced Settings	To use the functions listed in **Advanced Settings**, click **Configure now**. **IAM Agency**: Entrust a cloud service to perform professional and efficient O&M on IEC resources. If you have created an agency in IAM, select the agency from the drop-down list. If no agency has been created, click **Create Agency** to go to the IAM console to create one. Select **ECS_BMS** for **Cloud Service** when you create the agency For details about how to create an agency, see **Cloud Service Delegation**. If you need to select an agency after you have created the edge service, you can select an edge instance contained in the edge service, click the instance name to go to the **Summary** page, and select an agency in the **Agency Details** area.	Select **Configure now**. Select **IECAgency01**.

Step 3 Set Instance Distribution

Before setting instance distribution, you need to understand the concepts of edge sites and edge locations and as well as their **relationships**.

Configure the parameters based on **Table 3-2** and click **Next: Confirm Order**.

Table 3-2 Parameter description

Parameter	Description	Example Value
Geographic Level	IEC has one or more sites in each city where the lines of one or more carriers are deployed. You can choose to deploy edge instances at one site or multiple adjacent sites that are grouped based on the locations of these sites. There are three geographic levels for distributing edge instances at the sites: **City**, **Province**, and **Region**.	Region

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Distribution Policy	• **Centralized**: The system intelligently schedules multiple edge instances at the same site at the distribution level you select, so that these instances are close to one another. • **Dispersed**: The system intelligently schedules multiple edge instances at different sites at the distribution level you select, making them as dispersed as possible.	Centralized
Location and Quantity	Select the specific locations where your workloads will run and the carrier lines (or carriers), as well as the quantity of edge instances you require at the locations. Each location has one or more sites with the lines of different carriers deployed. • **Location**: indicates a specific city, province, or region, and the carrier line (or carrier). If you have enabled **Bind EIP**, you can view carrier lines and select one based on your requirements. – **City**: Select one or more cities and a carrier line for each city. The system will schedule the instances at the sites with the selected carrier line deployed in each city. – **Province**: Select one or more provinces and a carrier for each province. The system will schedule the instances at the sites with the lines of the selected carrier deployed in each province. – **Region**: Select one or more regions and a carrier for each region. The system will schedule the instances at the sites with the lines of the selected carrier deployed in each region. • **Quantity**: Set the number of edge instances you require at each location.	East China | China Mobile 3 East China | China Unicom 5

To learn more about instance distribution, see **Distributing Instances**.

Distribute edge instances based on your service distribution needs, latency requirements, and edge sites provided by IEC.

Copyright © Huawei Technologies Co., Ltd.

Step 4 Confirm the Order

Step 1 Check whether the edge instance configuration and distribution meet your service requirements.

Step 2 Confirm the price.

For details, see **Product Pricing Details**.

Step 3 Click **Buy Now**.

If you need to modify the information, click **Previous**.

----End

Related Operations

- Viewing an edge service

  You can view information about the edge services you create on the **Edge Services** page.

  For details, see **Viewing Edge Service Information**.

- Viewing an edge instance

  On the **Edge Services** page, locate the edge service that the edge instance you want to view belongs to, and click **View Edge Instance** in the **Operation** column. You can also click the edge service name to go to the details page and view the edge instance information.

  For details, see **Viewing an Edge Instance**.

- Logging in to an edge instance

  For details, see **Logging In to an Edge Instance**.

- Testing and deploying workloads on edge instances

  When an edge service and instances in it are running properly, you can test and deploy workloads on the instances you choose.

- Monitoring

  Server monitoring: View the performance metrics and running status of your edge instances.

  Viewing bandwidth and EIP monitoring data: View the metrics and alarms generated for bandwidths and EIPs at any time.

- Expanding an edge service

  For details, see **Expanding an Edge Service**.

- Deleting an edge service

  For details, see **Deleting an Edge Service**.

- Viewing task details

  If an edge service fails to be created, expanded, or deleted, you can view the task details to learn about the cause of failure and rectify the fault accordingly.

  In the edge service list, locate the edge service, click **More** in the **Operation** column, and select **View Task Details**.

Copyright © Huawei Technologies Co., Ltd.

3.3 Viewing Edge Service Information

Scenarios

After an edge service is created, you can view its information on the **Edge Services** page, including its name, ID, status, number of instances, and location.

You can also click its name to go to the details page and view more information, such as instance details.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Services**.

Step 4 View basic information about edge services on the edge service list page.

Table 3-3 Edge service information

Parameter	Description
Name/ID	• **Name**: edge service name that you entered during edge service creation. • **ID**: After an edge service is created, the system automatically generates an ID. The ID is globally unique and allows operations on IEC resources through APIs.
Status	Edge service status. Possible values are **Running**, **Being deployed**, **Deleting**, and **Failed**. The edge service status is **Being deployed** during edge service creation and subsequent capacity expansion.
Instances	Total number of edge instances in an edge service.
Distribution Level	The value is **City**, **Province**, or **Region**.
Region	Specific location where the instances are deployed, for example, Changsha city, Sichuan province, or North China.
Scheduling Policy	The value is either **Centralized** or **Dispersed**.

Step 5 (Optional) If an edge service fails to be created, expanded, or deleted, you can view the task details to learn about the cause of failure and rectify the fault accordingly.

Locate the edge service, click **More** in the **Operation** column and select **View Task Details**.

 Copyright © Huawei Technologies Co., Ltd.

Step 6 Locate the edge service, click its name to go to the details page, and view information such as the creation time and number of instances included in the edge service.

----End

3.4 Expanding an Edge Service

Scenarios

You can add edge instances to an edge service to expand its capacity.

Prerequisites

The edge service must be in the **Running** state.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

Step 3 In the navigation pane on the left, choose **Edge Services**.

The edge service list is displayed.

Step 4 Locate the edge service whose capacity you want to expand, click **More** in the **Operation** column, and select **Expand Capacity**.

Step 5 Add one or more edge instances to the edge service. For details, see steps 2 and 3 in **Creating an Edge Service**.

After capacity expansion is complete, check for the added edge instances.

----End

3.5 Deleting an Edge Service

Scenarios

You can delete an edge service that you no longer need.

Prerequisites

The edge service is in the **Running** or **Failed** state and does not contain any edge instances.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 In the navigation pane on the left, choose **Edge Services**.

The edge service list is displayed.

Step 4 Locate the edge service you want to delete, click **More** in the **Operation** column, and select **Delete**.

Step 5 Confirm the information and click **Yes**.

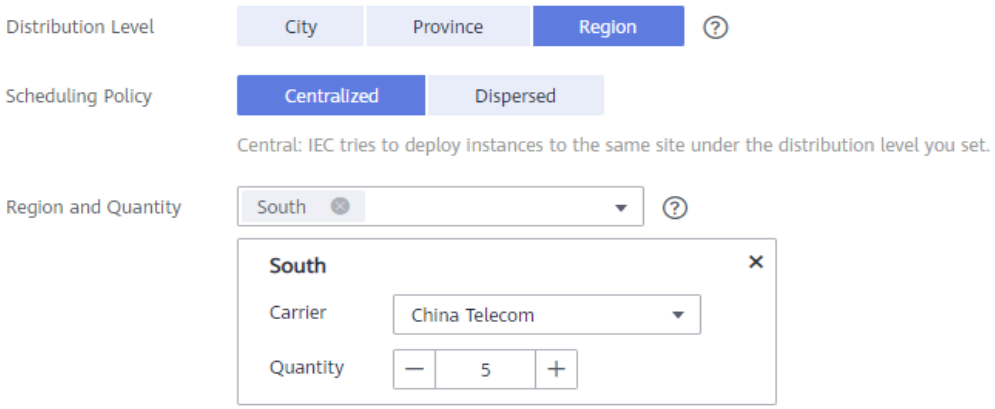
You can also select multiple edge services and click **Delete** above the edge service list.

----End

3.6 Examples of Edge Instance Distribution

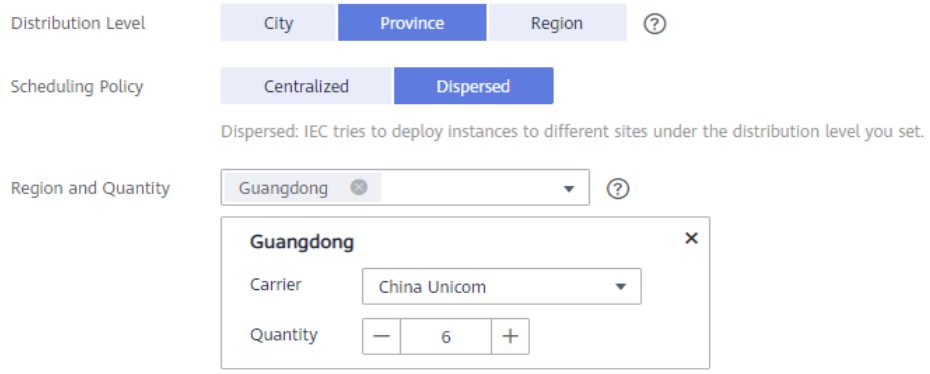
- Example 1: As shown in **Figure 3-3**, you choose to centrally deploy workloads on instances in South China and choose China Telecom as the carrier. The system will attempt to schedule the five edge instances to the edge sites in a city in a South China province.

  Figure 3-3 Example 1



- Example 2: As shown in **Figure 3-4**, you choose dispersed deployment for workloads in Guangdong province and choose China Unicom as the carrier. The system will schedule the six edge instances to edge sites in different cities in Guangdong province, to keep them away from one another.

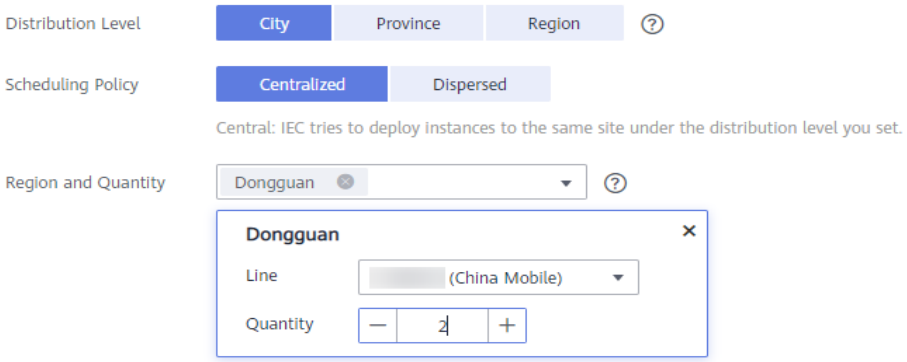
  Figure 3-4 Example 2



 Copyright © Huawei Technologies Co., Ltd.

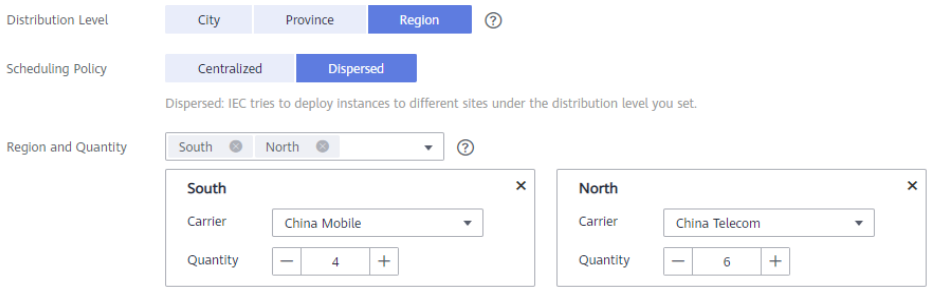
- Example 3: As shown in **Figure 3-5**, you choose to centrally deploy workloads on instances in Dongguan and choose China Mobile as the carrier. The system will attempt to schedule the two edge instances to the edge sites in Dongguan.

  Figure 3-5 Example 3

- Example 4: As shown in **Figure 3-6**, you choose dispersed deployment for workloads in South China and North China and choose China Mobile and China Telecom as carriers. The system will schedule four instances to edge sites in different cities of different provinces in South China and six instances to edge sites in different cities of different provinces in North China.

  Figure 3-6 Example 4

 Copyright © Huawei Technologies Co., Ltd.

4 Edge Instances

4.1 Edge Instance Overview

What Is an Edge Instance?

An edge instance is a compute resource dedicated to edge use. It includes vCPU, memory, OS, and disks.

Edge instances on IEC are independent of Elastic Cloud Servers (ECSs). The two run different services, but are similar in function.

Edge instances that you create on the IEC console or create by calling the IEC API belong only to IEC and are not related to ECSs that you create on the ECS console or create by calling the ECS API. You cannot manage IEC instances on the ECS console or manage them by calling the ECS API. Similarly, ECSs cannot be managed on IEC.

How to Use an Edge Instance?

An edge instance is automatically created when you **create an edge service** or **expand the capacity of an edge service**.

After an edge instance is created, you can use it as you would your local computer or a physical server to provide secure, reliable, and efficient computing.

IEC provides multiple edge instance types with different compute and storage capabilities. Each edge instance type provides various flavors with different vCPU and memory specifications for you to choose from.

- For details about edge instance types, see **Edge Instance Types**.
- For details about all edge instance statuses in a lifecycle, see **Edge Instance Lifecycle**.
- By default, you can use one HUAWEI CLOUD account to create a maximum of 50 edge instances. If you want to create more edge instances, increase the quota by referring to **Quota Adjustment**.
- By default, you can use one HUAWEI CLOUD account to create an edge instance with a maximum of 102,400 MB random access memory (RAM) and

 Copyright © Huawei Technologies Co., Ltd.

100 vCPUs. If you want more to user more RAM and vCPUs, increase the quota by referring to **Quota Adjustment**.

4.2 Edge Instance Lifecycle

A lifecycle indicates the possible edge instance statuses from the time you create the edge instance until the time you delete it.

Table 4-1 Edge instance statuses

Status	Attribute	Description
Creating	Intermediate	The edge instance has been created but is not running.
Starting	Intermediate	The edge instance is being started from the **Stopped** state, and its status will become **Running** after it is started.
Running	Stable	The edge instance is running properly. An edge instance in this state can run your services.
Stopping	Intermediate	The edge instance is being stopped from the **Running** state, and its status will become **Stopped** after it is stopped.
Stopped	Stable	The edge instance has been stopped. An edge instance in this state cannot provide services.
Frozen	Stable	Your HUAWEI CLOUD account is in arrears and is suspended by the system administrator. An edge instance in this state cannot provide services. The system retains it for a period of time. If it is not renewed after the time expires, the system will automatically delete it.
Restarting	Intermediate	The edge instance is being restarted.
Deleting	Intermediate	The edge instance is being deleted. If the edge instance remains in this state for a long time, there may be exceptions. In such a case, contact customer service.
Faulty	Stable	An error has occurred on the edge instance. An edge instance in this state cannot provide services. Contact customer service.
Changing OS	Intermediate	The OS of the edge instance is being changed.

Copyright © Huawei Technologies Co., Ltd.

Status	Attribute	Description
OS change Failed	Stable	The edge instance has received a request to change the OS, but the OS failed to change due to an exception. An edge instance in this state cannot provide services. Contact customer service.
Forcibly restarting	Intermediate	The edge instance is being forcibly restarted.
Locked by IMS	Intermediate	A private edge image is being created from the edge instance.
Locked	Intermediate/Stable	If  is displayed in the status bar, the edge instance is locked. In such a case, this edge instance will be protected, and certain operations on it will be forbidden. You can click the link below the lock icon to view the reason.

4.3 Edge Instance Types

IEC provides multiple types of edge instances for you to select. You can also configure different specifications as required.

Edge Instance Types

- General computing (S6)
- Memory-optimized (M6)
- General computing-plus (C6 and C6s)
- AI-accelerated (AI1)
- GPU-accelerated (G5r and PI2)
- Disk-intensive (D3i)

View specifications of each type of edge instance on the IEC console. For details about how to log in to the console, see **Creating an Edge Service**.

Flavor Naming Rules

AB.C.D

For example, *s2.medium.4*,

in which,

- **A** specifies the edge instance type and can be **s**, which is a general computing edge instance, **c**, which is a computing edge instance, or **m**, which is a memory-optimized edge instance.

  Kunpeng flavor names start with letter **k**. For example, **kc** indicates Kunpeng general computing-plus.

Copyright © Huawei Technologies Co., Ltd.

- **B** specifies the type ID. For example, the **1** in **s1** indicates a general first-generation ECS, and the **2** in **s2** indicates a general second-generation ECS.
- **C** specifies the flavor size, such as medium, large, xlarge, 2xlarge, 4xlarge, or 8xlarge.
- **D** specifies how many GiBs of memory are allocated for each vCPU. So for a flavor with 2 vCPUs, a value of 4 would mean it has 8 GiB (4 x 2) of memory.

On the IEC **Overview** page, you can click **Edge Instances** in the **My Resources** area to view the specifications of the created edge instances.

4.4 Viewing Edge Instance Information

Scenarios

After an edge instance is created, you can view its information on the IEC console.

In the edge instance list, view the edge instance name/ID, edge service it belongs to, site, status, specifications, images, EIP, and private IP address.

On the edge instance details page, view its basic information, billing information, disk, NIC, security group, EIP, and monitoring data.

You can also view the edge instance quantity changes over time on the IEC **Overview** page.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Instances**.

Step 4 On the **Edge Instances** page, view basic information about each edge instance.

 Copyright © Huawei Technologies Co., Ltd.

Table 4-2 Basic information

Parameter	Description
Name/ID	• **Name**: edge instance name. When you create an edge instance, the system will automatically add a prefix and a suffix to the instance name to differentiate instances. Naming format: IEC-*City name-Customized instance name-4 digit suffix* (ascending order) Example: **IEC-beijing01-resource-0001** **IEC-beijing01-resource-0002** **IEC-beijing01-resource-0003** Policy for processing special characters in city names (city names indicates instance locations): – Spaces will be deleted. For example, **wu han** is changed to **wuhan**. – Apostrophes (') or backticks (') will be replaced by underscores (_). For example, **xi'an** is changed to **xi_an**. – Phonetic symbols will be deleted. For example, **ürümqi** is changed to **urumqi**. • **ID**: After an edge instance is created, the system automatically generates an ID. The ID is globally unique and allows operations on IEC resources through APIs.
Edge Service	Name of the edge service the edge instance belongs to.
Region	Specific location of the edge site to which the edge instance belongs
Status	Edge instance status. For details about all statuses, see **Edge Instance Lifecycle**.
Specifications/ Image	Specifications and images of the edge instance.
IP Address	• EIP: the EIP bound to the edge instance. • Private IP address: the private IP address the system automatically assigns to an edge instance when you create the instance.

Step 5 (Optional) Click go to the **Task Details** page and view the cause of failure if an edge instance fails to be created.

 Copyright © Huawei Technologies Co., Ltd.

Step 6 Click the name of the edge instance you want to view. On the displayed page, view its basic information, billing information, disk, NIC, security group, EIP, and **monitoring data**.

----End

4.5 Logging In to an Edge Instance

Scenarios

After you **create an edge service** or **expand the capacity of an edge service**, you can log in to any edge instance that is automatically created by the system.

This section describes how to log in to a Linux edge instance using an SSH password.

- **Logging In to the Linux Edge Instance from Local Windows**
- **Logging In to the Linux Edge Instance from Local Linux**

Prerequisites

- You have **bound an EIP** to the edge instance.
- The target edge instance must be in the **Running** state.
- You have allowed access to port 22 in the inbound direction of the security group that the edge instance is associated with. For details, see **Configuring Security Group Rules** and **Enabling Remote SSH Access to Linux Edge Instances**.
- You have enabled Internet Control Message Protocol (ICMP) in the inbound direction of the security group that the edge instance is associated with. For details, see **Configuring Security Group Rules** and **Pinging an Edge Instance from a Public Network**.
- The network connection between the login tool (PuTTY) and the target edge instance is normal. For example, the default port 22 is not blocked by a firewall.

Constraints and Limitations

You cannot use Virtual Network Console (VNC) to log in to edge instances. You must use a remote connection tool.

Logging In to the Linux Edge Instance from Local Windows

The following operations use PuTTY as an example.

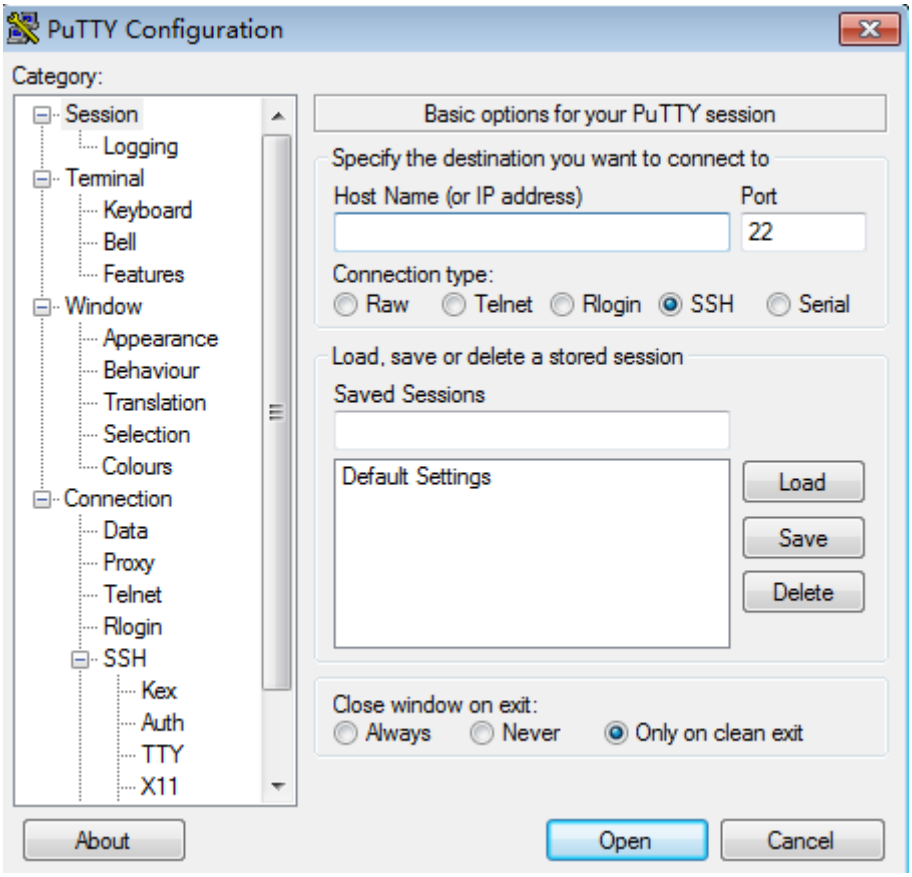
1. Visit this website and download PuTTY and PuTTYgen:
   https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
2. Run PuTTY.
3. Click **Session**.
   a. **Host Name (or IP address)**: EIP bound to the edge instance
   b. **Port**: **22**

Copyright © Huawei Technologies Co., Ltd.

c. **Connection type**: **SSH**

d. **Saved Sessions**: task name, which can be clicked for remote connection when you use PuTTY the next time

Figure 4-1 Session



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

   If you are logging in to the edge instance for the first time, PuTTY displays a security warning dialog box, asking if you want to accept the edge instance security certificate. Click **Yes** to save the certificate to your local registry.
6. After the SSH connection to the edge instance is set up, enter the username and password to log in to the edge instance.

Logging In to the Linux Edge Instance from Local Linux

On the CLI of your computer, run this command to log in to the edge instance:

ssh *EIP bound to the edge instance*

Copyright © Huawei Technologies Co., Ltd.

4.6 Managing an Edge Instance

Scenarios

After an edge instance is created, you can perform routine management operations on it, such as **starting, stopping, or restarting an edge instance**, **deleting an edge instance**, **changing the OS of an edge instance**, **changing the name of an edge instance**, **adding a NIC to an edge instance**, or **binding an EIP to an edge instance**.

Starting, Stopping, or Restarting an Edge Instance

1. Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

   The IEC **Overview** page is displayed.

2. In the navigation pane on the left, choose **Edge Instances**.
3. On the **Edge Instances** page, locate the edge instance, and choose **Start**, **Stop**, or **More** > **Restart** in the **Operation** column.

   Alternatively, click the edge instance name. On the displayed details page, click **Start**, **Stop**, or **Restart** in the upper right corner.

   To start, stop, or restart edge instances in batches, select multiple edge instances and click **Start**, **Stop**, or **Restart** above the edge instance list.
4. In the displayed dialog box, click **Yes**.

Deleting an Edge Instance

1. Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

   The IEC **Overview** page is displayed.

2. In the navigation pane on the left, choose **Edge Instances**.
3. In the edge instance list, locate the edge instance you want to delete, click **More** in the **Operation** column, and select **Delete**.

   To delete edge instances in batches, select multiple edge instances and click **Delete** above the edge instance list.

   Deleted edge instances cannot be recovered. Exercise caution when performing this operation.
4. In the displayed dialog box, click **Yes**.

Changing the OS of an Edge Instance

If you change the OS, the system will automatically change the system disk attached to the edge instance. After you change the OS, the system assigns a new ID to the system disk of the edge instance and deletes the original system disk.

For details, see **Changing the Edge Instance OS**.

 Copyright © Huawei Technologies Co., Ltd.

Creating a Private Image

Use an edge instance to create an IEC private image. The image will contain custom functions you have configured, saving the time for repeated configuration.

1. Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

   The IEC **Overview** page is displayed.
2. In the navigation pane on the left, choose **Edge Instances**.
3. In the edge instance list, locate the edge instance you want to use to create an IEC private image, click **More** in the **Operation** column, and select **Create Image**.
4. For details, see **Using an Edge Instance to Create an IEC Private Image**.

Changing a Security Group

Change the security group to which the NIC of an edge instance belongs as required.

For details, see **Changing a Security Group**.

Changing the Name of an Edge Instance

1. Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

   The IEC **Overview** page is displayed.
2. In the navigation pane on the left, choose **Edge Instances**.
3. In the edge instance list, locate the edge instance you want to modify and click  next to the edge instance name.

   The name can contain 1 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
4. Click **OK** to save the modification.

Adding a NIC to an Edge Instance

1. Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

   The IEC **Overview** page is displayed.
2. In the navigation pane on the left, choose **Edge Instances**.
3. Click the name of the edge instance to which you want to add a NIC.

   The **Summary** tab page is displayed.
4. Click the **NICs** tab.
5. Click **Add NIC**.

   The **Add NIC** dialog box is displayed.
6. Select a security group and specify the number of NICs you want to add.

   Each NIC of an edge instance corresponds to a subnet.
7. Click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Related Operations

- **Configuring policy-based routing for an edge instance with multiple NICs**
- **Accessing the Internet using an EIP bound to an extension NIC**

Binding an EIP to an Edge Instance

An edge instance can have multiple NICs, and each NIC can have an EIP bound to it.

1. Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.
   The IEC **Overview** page is displayed.
2. In the navigation pane on the left, choose **Edge Instances**.
3. Click the name of the edge instance to which you want to bind an EIP.
   The **Summary** tab page is displayed.
4. Click the **EIPs** tab.
5. Click **Bind EIP**.
   The **Bind EIP** dialog box is displayed.
6. Select a NIC.
7. Select an EIP.
8. Click **OK**.

4.7 Changing the Edge Instance OS

Scenarios

If you change the OS, the system will automatically change the system disk attached to the edge instance. After you change the OS, the system assigns a new ID to the system disk of the edge instance and deletes the original system disk.

If the OS running on an edge instance cannot meet your service requirements, you can change the edge instance OS.

IEC enables you to change an edge instance OS based on an image to another image of the same type or a different type (public image and private image).

Constraints and Limitations

- After you change the OS, the system will not retain the original OS, and deletes the original system disk.
- Back up necessary data. When you change the OS, the system will clear data in all partitions of the system disk, including the system partition.
- Changing the OS will not affect data in data disks.
- After you change the OS, you must deploy your service running environment in the new OS again.
- After you change the OS, the edge instance will be automatically started.
- After you change the OS, you cannot change the system disk type of the edge instance.

 Copyright © Huawei Technologies Co., Ltd.

- After you change the OS, the IP and MAC addresses of the edge instance remain unchanged.
- After you change the OS, customized configurations, such as DNS and hostname of the original OS will be reset and require reconfiguration.
- It takes about 10 to 20 minutes to change the OS. During this process, the edge instance will be in the **Changing OS** state.
- You cannot switch between edge instances in BIOS boot mode and UEFI boot mode.
- The disk quota must be greater than 0.

Notes on OS Change

OS change involves changing between Windows and Linux.

- To change Windows to Linux, install an NTFS partition tool, such as NTFS-3G for data reading and writing data on the Windows edge instance.
- To change Linux to Windows, install software, such as Ext2Read and Ext2Fsd to identify ext3 or ext4.

  It is recommended that you do not change Linux to Windows on the cloud platform. If there are LVM partitions on the Linux edge instance, these partitions may fail after you change the OS to Windows.

Prerequisites

- You have stopped the edge instance whose OS you want to change.
- The target edge instance has a system disk attached.
- If you require a private image to change the edge instance OS, create the desired private image by following the instructions provided in the **Image Management Service User Guide**.
  - If you require the image of a specific edge instance, make sure that you have created a private image using the edge instance.
  - If you require a local image file, make sure that you have imported the image file to the cloud platform and registered it as a private image.
  - If you required a private image from another region, make sure that you have copied the image to the target region.
  - If you require a private image from another account, make sure that the account has shared the image with you.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Instances**.

Step 4 Locate the edge instance whose OS you want to change, click **More** in the **Operation** column, and select **Change OS**.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Modify related edge instance parameters, such as **Image Type** and **Image**, based on service requirements.

For details about related parameters, see **Step 2 Configure Edge Instances**.

Step 6 Set **Login Mode**.

Step 7 Click **OK**.

Step 8 On the **Resource Details** page, confirm the configurations and click **Submit Application**.

After you submit the application, the edge instance status changes to **Changing OS**. The process of changing the OS will be completed when **Changing OS** disappears.

----End

Follow-up Procedure

- If the OS before and after the OS change is Linux, and you have enabled automatic partition mounting upon system startup for the data disk, the data disk partition mounting information will be lost after the OS is changed. In this case, you need to update the **/etc/fstab** configuration.
  a. Write the new partition information into **/etc/fstab**.
     It is recommended that you back up the **/etc/fstab** file before you write data into it.
  b. Mount the partition so that you can use the data disk.
     mount *Disk partition Device name*
  c. Check the mount result.
     df -TH
- If the OS change is unsuccessful, repeat **Procedure** to change the OS.
  If the second OS change attempt is unsuccessful, contact customer service for manual recovery at the backend.

4.8 Creating a Key Pair

Scenarios

To ensure system security, it is recommended that you use the key pair authentication mode to authorize users who will log in to an edge instance. Therefore, you must use an existing key pair or create one for remote login authentication.

- Creating a key pair
  If no key pair is available, create a key pair in which the private key can be used for login authentication. You can create a key pair using either of the following methods:
  – (Recommended) Create a key pair on the management console. After you create the key pair, the public key will be automatically stored in the system, and you need to store the private key in a local directory. For details, see **Creating a Key Pair on the Management Console**.

 Copyright © Huawei Technologies Co., Ltd.

  - Create a key pair using **puttygen.exe**. After you create the key pair, you need to store both the public key and private key locally. For details, see **Creating a Key Pair Using puttygen.exe**. After you create the key pair, import it by following the instructions provided in **Importing a Key Pair**. Then, you can use the key pair.

- Using an existing key pair

  If a key pair is available locally, for example, generated using PuTTYgen, you can import the public key on the management console so that the system maintains the public key file. For details, see **Importing a Key Pair**.

  If you have stored the public key of the existing key pair by clicking **Save public key** of **puttygen.exe**, you cannot import the public key to the management console. Troubleshoot the issue and then use this key pair for remote authentication. For details, see **Troubleshooting the Issue that a Key Pair Created Using puttygen.exe Cannot Be Imported to the Management Console**.

Constraints and Limitations

- The following encryption algorithms are supported:
  - SSH-2 (RSA, 1024)
  - SSH-2 (RSA, 2048)
  - SSH-2 (RSA, 4096)
- The private key is one of the most important methods to protect your edge instances during the remote login. To ensure edge instance security, the private key can be downloaded only once. Therefore, keep it secure.

Creating a Key Pair on the Management Console

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

Step 3 In the navigation pane on the left, choose **Key Pairs**, and click **Create Key Pair**.

Step 4 Enter the key pair name and click **OK**.

An automatically allocated key pair name consists of **KeyPair-** and a 4-character random number. Change it to a name that is easy to remember, for example, **KeyPair-xxxx_iec**.

Step 5 Download the private key file. The file name will be the key pair name you specify with the suffix **.pem**. Store the private key file in a secure path. In the displayed **Information** dialog box, click **OK**.

You can download the private key file only once, so keep it secure. When you create an edge service, provide the name of your key pair. Each time you log in to the edge instance using SSH, you will need to provide the private key.

----End

 Copyright © Huawei Technologies Co., Ltd.

Creating a Key Pair Using puttygen.exe

Step 1 Download and install PuTTY and PuTTYgen.

https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

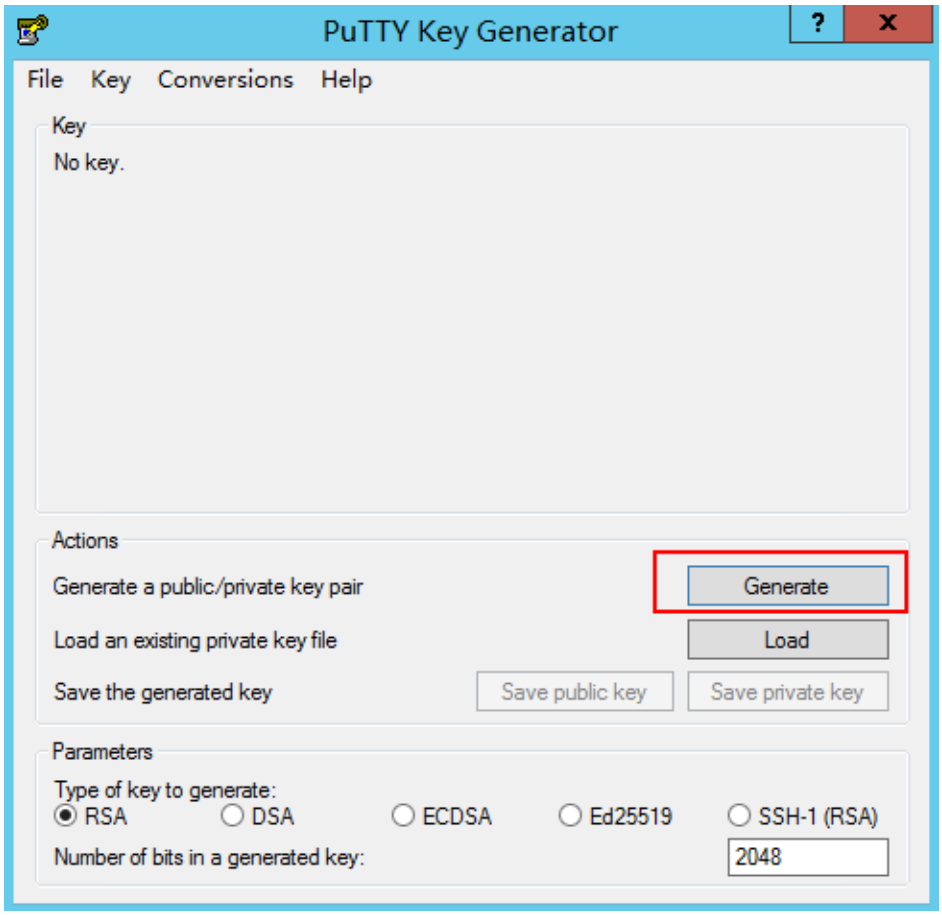
NOTE

PuTTYgen is a key generator, which you can use to create a key pair that contains a public key and a private key for PuTTY.

Step 2 Obtain the public and private keys.

1. Double-click **puttygen.exe** to switch to the **PuTTY Key Generator** page.

Figure 4-2 PuTTY Key Generator

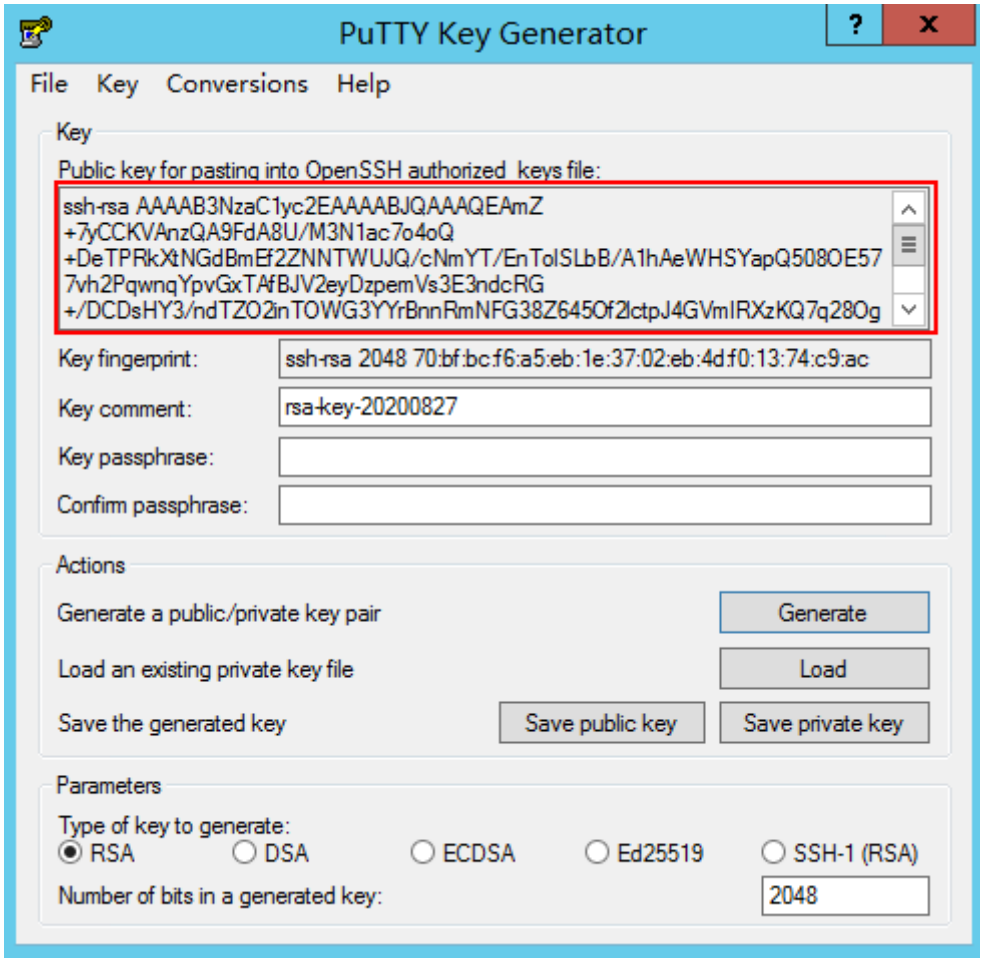


2. Click **Generate**.

   The key generator automatically generates a key pair that contains a public key and a private key. The public key is shown in the red box in **Figure 4-3**.

Copyright © Huawei Technologies Co., Ltd.

Figure 4-3 Obtaining the public and private keys



Step 3 Copy the public key content and paste it to a .txt file and save the file in a local directory.

NOTE

Do not save the public key by clicking **Save public key**. Storing a public key by clicking **Save public key** of **puttygen.exe** will change the format of the public key content. You cannot import such a key to the management console.

Step 4 Save the private key file.

The format in which to save your private key varies depending on application scenarios. To ensure the security of your edge instance, you can only download the private key once.

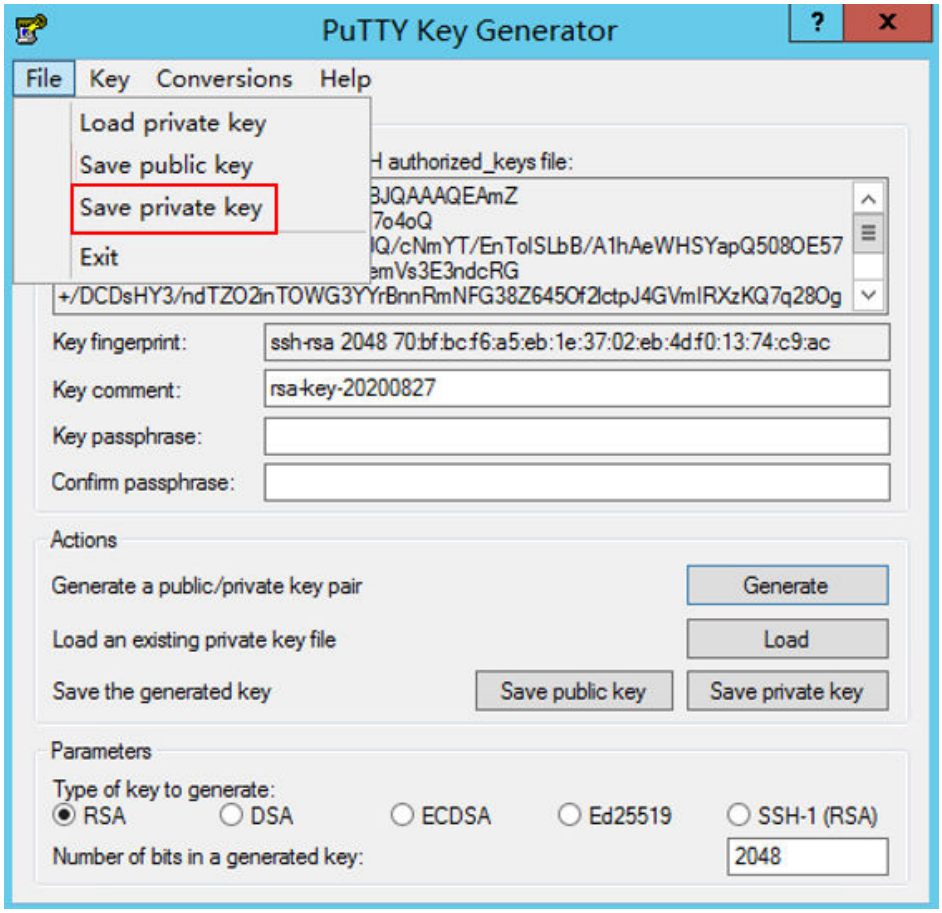
- Saving the private key in .ppk format

  When you log in to a Linux edge instance using PuTTY, you must use the .ppk private key. To save the private key in .ppk format, perform the following operations:

  a. On the **PuTTY Key Generator** page, choose **File** > **Save private key**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-4 Save private key



b. Save the converted private key, for example, **kp-123.ppk**, to your local PC.

- Saving the private key in .pem format

  When you log in to a Linux edge instance using Xshell or attempt to obtain the password for logging in to a Windows edge instance, you must use the **.pem** private key for authentication. To save the private key in .pem format, perform the following operations:

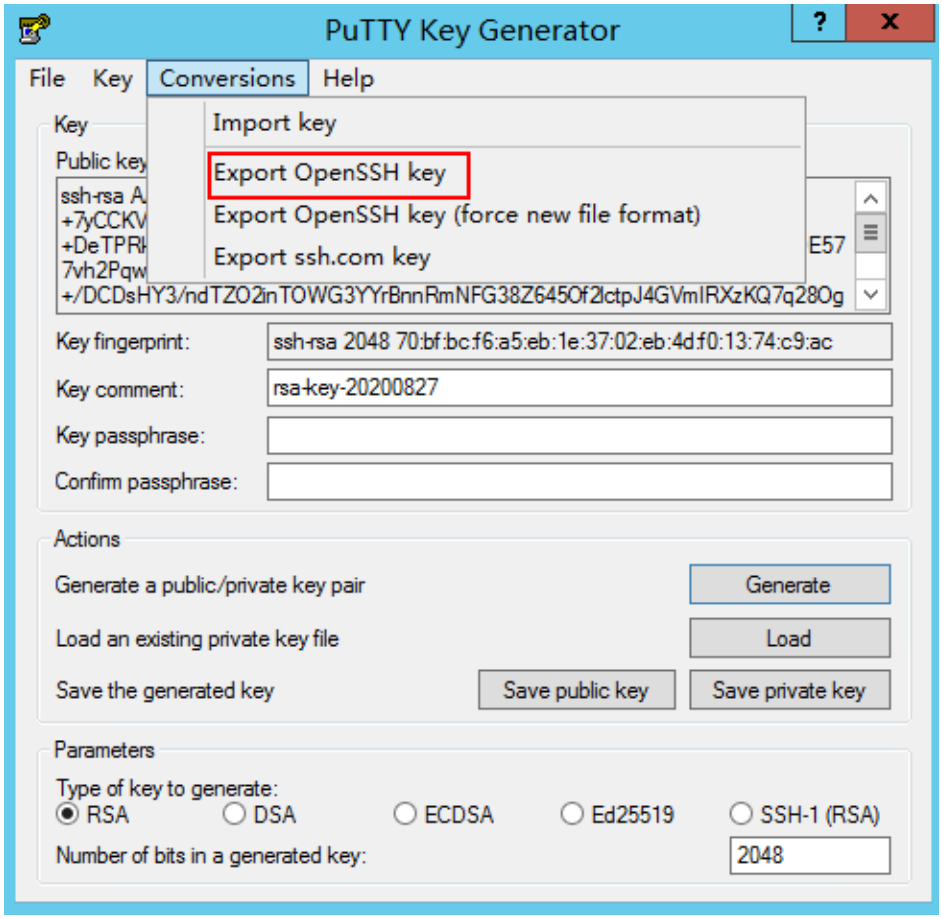
  a. Choose **Conversions** > **Export OpenSSH key**.

  NOTICE

  If you intend to use this private file to obtain the password for logging in to a Windows edge instance, when you choose **Export OpenSSH key**, do not configure **Key passphrase**. Otherwise, you cannot obtain the password.

Copyright © Huawei Technologies Co., Ltd.

Figure 4-5 Export OpenSSH key



b. Save the private key, for example, **kp-123.pem**, to your local PC.

Step 5 Import the public key to the system. For details, see "Copying the public key content" in **Importing a Key Pair**.

----End

Importing a Key Pair

If you store a public key by clicking **Save public key** of **puttygen.exe**, the format of the public key content will change. You cannot import such a key to the management console. Therefore, obtain the public key content in the correct format and import the content to the management console. For details, see section **Troubleshooting the Issue that a Key Pair Created Using puttygen.exe Cannot Be Imported to the Management Console**.

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

Step 3 In the navigation pane on the left, choose **Key Pairs**.

Step 4 On the right pane, click **Import Key Pair**.

Step 5 Use either of the following methods to import the key pair:

 Copyright © Huawei Technologies Co., Ltd.

- Selecting a file
  a. On the **Import Key Pair** page of the management console, click **Select File** and select the local public key file, for example, the .txt file saved in **Step 3**.

     When you import a key pair, ensure that the public key is imported. Otherwise, the importing will fail.
  b. Click **OK**.

     After you import the public key, you can change its name.
- Copying the public key content
  a. Copy the content of the public key in .txt file into the **Public Key Content** text box.
  b. Click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

5 Edge Images

5.1 Edge Image Overview

An image is an instance template that contains an OS or service data and may also contain private software and application software, such as database software.

IEC edge images can be public or private images.

Table 5-1 Image types

Image Type	Overview	How to Use
Public image	A public image is a standard, widely used image. It contains an OS and preinstalled public applications and is available to all users. You can configure the application environment and software for your edge instances as needed. Preset IEC public images are independent of **IMS** as you cannot manage them on IMS. You cannot manage IMS public images on IEC. Public images cannot be modified.	You can directly use the IEC public images on the IEC console. If the public images provided by IEC do not meet your requirements, you can create private images or contact customer service and request for images you require.

 Copyright © Huawei Technologies Co., Ltd.

Image Type	Overview	How to Use
Private image	You can create a private image from an existing running instance or import one from an external system. A private image contains an OS, pre-installed public applications, and owner's private applications. Only the creator of a private image can use the image. If you use a private image to create edge instances, you do not need to configure multiple edge instances repeatedly.	IEC provides two image sources: IMS and edge instance. • IMS: You can create a private image on **IMS** or select an existing IMS private image and use the created or selected private image to create an IEC private image on the IEC console. An IEC private image that you create from an IMS private image is independent of the IMS private image. Modifications to the IMS private image do not affect the IEC private image. An IEC private image that you create cannot be modified. If an IEC private image does not meet your requirements, you can create a new one. • Edge instance: If you already have an edge instance (created during **edge service creation**) and you have configured it (software installation and application environment deployment configuration) based on your service requirements, you can create an IEC private image from the edge instance.

5.2 Using IMS to Create an IEC Private Image

Scenarios

You can use an **IMS** private image to create an IEC private image.

- If the private image is available on IMS, select the private image on the IEC console to create an IEC private image.
- If the private image is unavailable on IMS, create it on IMS and then select the created IMS private image on the IEC console to create an IEC private image.

This section uses the second scenario as an example.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

You have **made preparations** for using IMS.

Constraints and Limitations

- You can use IMS to create IEC private images only in the **CN North-Beijing4** region.
- If an IAM user uses IMS to create a private edge image, the account must be granted the **IEC FullAccess** permission and the **IAM ReadOnlyAccess** permission in the **CN North-Beijing4** region.
- By default, you can use one HUAWEI CLOUD account to create a maximum of 50 IEC private images (created from both edge instances and IMS). If you want to create more IEC private images, increase the quota by referring to **Quota Adjustment**.

Procedure

Step 1 Log in to the IMS console and create a private image.

For details about how to create a Linux system disk image, see the following:

- **Creating a System Disk Image from a Linux ECS**
- **Creating a Linux System Disk Image from an External Image File**
- **Creating a Linux System Disk Image from an ISO File**

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Images**, and click **Create Private Image** in the upper right corner.

Step 4 On the **Create IEC private image** page, select **IMS** for **Source**.

Step 5 Select the required region and private image.

Step 6 Confirm the parameters. Read and select the check box, and click **Create Now**.

Step 7 Go back to the IEC private image list and view the image status.

The time required for creating an image depends on the image file size, network status, and number of concurrent tasks. When the image status changes to **Normal**, the image is created successfully.

----End

5.3 Using an Edge Instance to Create an IEC Private Image

Scenarios

If you already have an edge instance (created during **edge service creation**) and you have configured it (software installation and application environment

Copyright © Huawei Technologies Co., Ltd.

deployment configuration) based on your service requirements, you can create an IEC private image from the edge instance. The system will apply the configurations to all the new edge instances that you create based on this image.

A Linux edge instance is used as an example to describe how to create a Linux system image.

Prerequisites

- Delete sensitive data from the edge instance to prevent data leak.
- Ensure that the edge instance is in the **Running** or **Stopped** state. When you create the private image, do not stop, start, or restart the edge instance. Otherwise, the image creation may fail.
- Check network configuration of the edge instance and ensure that DHCP is configured for the NICs (default for an edge instance).
- Delete network rule files to prevent NIC name drift on the edge instances created from the image. For details, see **Deleting Files in the Network Rule Directory**.
- If multiple data disks are attached to the edge instance that you use to create an IEC private image, and you use the IEC private image to create edge instances, these edge instances may not be available. Detach all data disks from the edge instance before you use it to create a private image. For details, see **Detaching Data Disks from an Edge Instance**.

Constraints and Limitations

By default, you can use one HUAWEI CLOUD account to create a maximum of 50 IEC private images (created from both edge instances and IMS). If you want to create more IEC private images, increase the quota by referring to **Quota Adjustment**.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Images**, and click **Create Private Image** in the upper right corner.

Step 4 On the **Create Private Image** page, select **Edge Instance** for **Source**.

Step 5 Select an edge instance that has been **initialized** from the list.

If no appropriate edge instance is available, click **Create Edge Service** to create an edge instance.

Step 6 In the **Image Information** area, set **Name** to an image name that is easy to identify.

Step 7 Confirm the parameters. Read and select the check box, and click **Create Now**.

 Copyright © Huawei Technologies Co., Ltd.

Step 8 Go back to the IEC private image list and view the image status.

The time required for creating an image depends on the size of the edge instance system disk, network status, and number of concurrent tasks. When the image status changes to **Normal**, the image is created successfully.

----End

Follow-up Operations

After you create the system disk image, you can use the image to create an edge instance or change the OS of an existing edge instance to migrate data between the two edge instances. For details, see

- **Creating an edge service**
- **Changing the edge instance OS**

5.4 Viewing Edge Image Information

Scenarios

On the **Edge Images** page, view information about public images and registered private images, such as the image name and status, so that you can select appropriate images to create edge services if needed.

Public Images

Table 5-2 Parameter description

Parameter	Description
Name	Public image name, which is automatically generated by the system.
Status	Public image status. The status can be **Normal** or **Error**. • You can use a public image in the **Normal** state. Click **Create Edge Service** in the **Operation** column to use the image to create an edge service. • You cannot use a public image in the **Error** state.
OS	OS used by the edge instance. Public images support mainstream Linux OSs, such as Ubuntu and CentOS. Public image OSs are pre-configured.
Image Type	A system disk image with a default configuration.
Disk Capacity (GB)	System disk capacity of the public image.

Copyright © Huawei Technologies Co., Ltd.

Private Images

Table 5-3 Parameter description

Parameter	Description
Name	IEC private image name, which was set on the IMS console.
Status	Private image status. The status can be **Normal**, **Creation failed**, or **Creating**. • **Normal**: The private image can be used properly. You can click **Create Edge Service** in the **Operation** column to use the image to create an edge service. • **Creation failed**: The image creation failed. You can click **Recreate** in the **Operation** column to create the private image again. • **Creating**: This is an intermediate state.
OS	OS used by the IEC private image, which was set on the IMS console.
Image Type	IEC private image type, which was set on the IMS console.
Disk Capacity (GB)	System disk capacity of the IEC private image, which was set on the IMS console.
Created	Time when the private image was created on the IEC console.

5.5 Deleting an IEC Private Image

Table 5-4 Deletion description

Image Type	Description
Public image	Public images cannot be deleted.
Private image	To delete an IEC private image on the IEC console, choose **Edge Images**, click **Private Images**, locate the image, and click **Delete** in the **Operation** column. **NOTE** To delete multiple private images, select the private images you want to delete and click **Delete** in the upper left corner of the list. Deleting a private image on the IEC console will not delete the source private image on the IMS console.

Copyright © Huawei Technologies Co., Ltd.

6 Edge Networks

6.1 Edge Network Overview

Scenarios

Edge networks are dedicated for an edge cloud. In the context of IEC, edge networks include VPCs and EIPs. A VPC is an isolated, configurable, and manageable virtual network environment. It improves the cloud resources security and simplifies network deployment. You can bind EIPs to edge instances in a VPC to allow them to access the Internet and access other cloud services in the central region from IEC over the Internet.

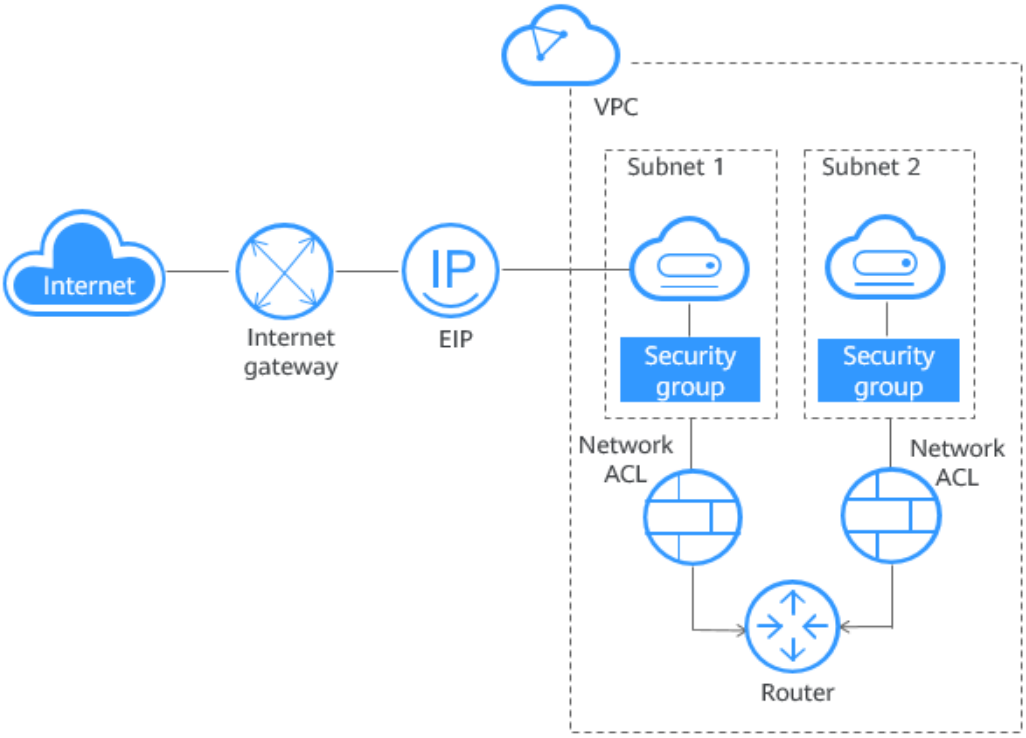
Edge networks are independent of network services in the central region such as Virtual Private Cloud (VPC) and Elastic IP (EIP). Edge networks network services in the central region have similar functions but are used in different scenarios.

For example, a VPC that you create on the IEC console or by calling IEC APIs belongs only to IEC and is not related to a VPC you create on the VPC console. A VPC that you create on IEC cannot be managed by using the VPC service, and a VPC that you create on the VPC console cannot be managed by using IEC.

Figure 6-1 shows the edge network architecture.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-1 Edge network architecture



VPCs

A VPC provides an isolated virtual network for your cloud resources. You can configure and manage the networks in the VPC, making changes to these networks quickly and securely.

Each VPC consists of a private CIDR block and at least one subnet. VPCs are logically isolated from each other and cannot communicate with each other.

- CIDR block

  When you create a VPC, you need to specify a CIDR block for the VPC.

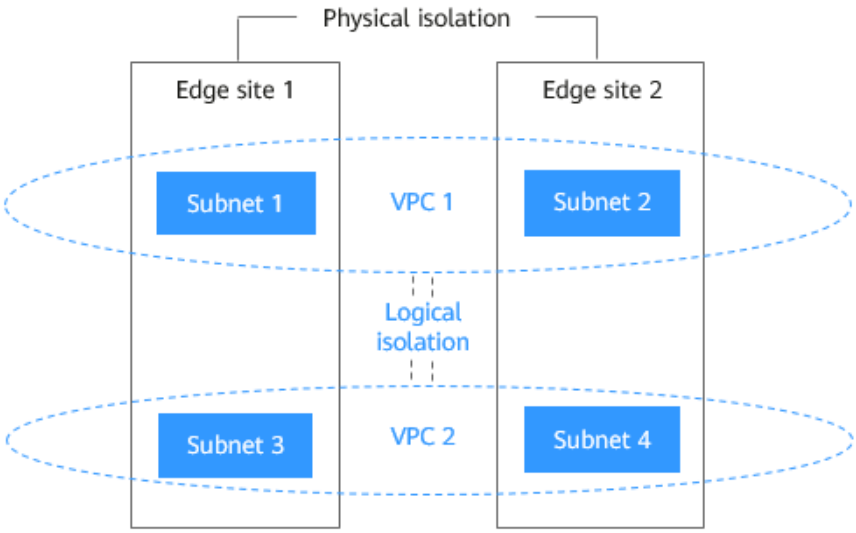
- Subnet

  A subnet is a range of IP addresses in your VPC. Edge cloud resources, such as edge instances, must be deployed in subnets. The IP addresses of all edge instances belong to the subnet. The subnet CIDR block must be within the private CIDR block. A VPC can be divided into one or more subnets. Subnets can be distributed across edge sites. However, subnets belonging to different edge sites are not connected because the edge sites are physically isolated.

  As shown in **Figure 6-2**, the four subnets are isolated from each other due to logical isolation of the VPCs and physical isolation of the edge sites.

Copyright © Huawei Technologies Co., Ltd.

Figure 6-2 Network connections among VPCs, subnets, and edge sites



Virtual IP Addresses

A virtual IP address is an IP address that is not allocated to an edge instance NIC. An edge instance can have both private and virtual IP addresses, and you can access the edge instance through either one. A virtual IP address has the same network access capabilities as a private IP address, including normal communication in VPCs and Internet access through EIPs.

A virtual IP address can be bound to only one edge instance.

NICs

A NIC is a type of virtual adapter that you can bind to an edge instance in a VPC. Through the NIC, you can manage edge instance network. A NIC can be a primary NIC or an extension NIC.

- Primary NIC

  When you create an edge instance, the NIC that is automatically created with the instance is the primary NIC. You cannot unbind the primary NIC. It is preferentially used for the default route generally.

- Extension NIC

  A NIC that you can add separately is an extension NIC. You can bind or unbind an extension NIC from an edge instance. When you create an edge instance, you can determine whether you want to add NICs and the number of NICs you want to add.

Route Tables

A route table contains a set of rules, called **routes**, that are used to control where inbound and outbound subnet traffic is forwarded within a VPC. A route table can

 Copyright © Huawei Technologies Co., Ltd.

have multiple subnets associated with it. However, each subnet can be associated with only one route table.

When you create a VPC, a default route table will be generated for the VPC. When you create an edge service, the system will automatically allocate a subnet for the edge instance in the VPC you select, and this subnet will be automatically associated with the default route table of the VPC. Default route tables are currently not displayed on the IEC console. If you do not want to use the default route table, you can now create a custom route table and associate it with the subnet.

The custom route table associated with a subnet affects only the traffic in the outbound direction, while the default route table determines the traffic in the inbound direction.

Route

A route is configured with the destination, next hop type, and next hop to determine where the network traffic is directed. Routes are classified into system routes and custom routes.

- System route: Routes that are automatically added by the system and cannot be modified or deleted.

  After a route table is created, the system automatically adds the following system routes to the route table, so that instances in a VPC can communicate with each other.

  - Routes whose destination is 100.64.0.0/10 or 198.19.128.0/20.
  - Routes whose destination is a subnet CIDR block.

  In addition to the preceding system routes, the system automatically adds a route whose destination is 127.0.0.0/8. This is the local loopback address.
- Custom route: A route that can be modified and deleted. The destination of a custom route cannot overlap with that of a system route.

  You can add a custom route and configure the destination, next hop type, and next hop in the route to determine where the network traffic is directed.

  Currently, IEC supports the following next hop types:

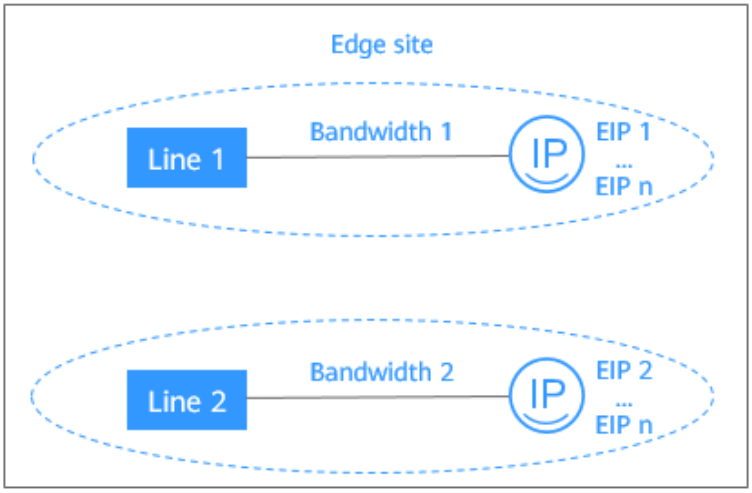
  - Edge instance: The traffic destined for the destination will be forwarded to an edge instance in the VPC.
  - Virtual IP address: The traffic destined for the destination will be forwarded to a virtual IP address bound to an edge instance.

Bandwidths

IEC provides edge site-level bandwidth sharing and multiplexing capabilities. All EIPs using the same carrier line share the same bandwidth. Different carrier lines use different bandwidths. Shared bandwidth reduces network operations costs and makes O&M statistics easier.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-3 Relationship between bandwidth, EIP, and line



After you assign an EIP, if the carrier line using the EIP does not have a shared bandwidth allocated to it, the system automatically allocates a shared bandwidth to it. Different carrier lines use different bandwidths.

EIPs

An EIP is a public IP address that is used to access the Internet. You can bind an EIP to or unbind an EIP from an edge instance or a virtual IP address.

However, you can bind an EIP to only one edge instance or virtual IP address that is in the same site as the EIP.

Security Groups

A security group is a collection of access control rules for edge instances that have the same security protection requirements and are mutually trusted within a VPC. After you create a security group, you can create different access rules (outbound and inbound rules) for the security group. These rules will apply to any edge instance that you add to this security group.

Network ACLs

A network ACL is an optional layer of security for your subnets. You associate one or more subnets with a network ACL. The network ACL can help control traffic in and out of the subnets.

Similar to security groups, network ACLs control access to the network. They add an additional layer of defense to your VPC. Security groups only have the "allow" rules, but network ACLs have both "allow" and "deny" rules. You can use network ACLs together with security groups to implement access control that is both comprehensive and fine-grained. For more information, see **Differences Between Security Groups and Network ACLs**.

Network ACLs can be used in the following scenarios:

 Copyright © Huawei Technologies Co., Ltd.

- If you want the application layer to provide services for users, you must allow traffic to reach the application layer from all IP addresses. However, you also need to prevent illegal access from malicious users. You can add network ACL rules to deny access from suspect IP addresses.
- If you want to isolate a port that has vulnerabilities, for example, port 445 that can be exploited by the WannaCry worm, you can add network ACL rules to deny access traffic from specific port and protocol, for example, TCP port 445.
- If you do not want defense for communication within a subnet, but require access control for communication between subnets, you can add network ACL rules to control traffic between subnets.
- If you have frequently accessed applications, you may need to adjust the security rule sequence to improve performance. A network ACL allows you to adjust the rule sequence so that you can apply frequently used rules before other rules.

6.2 VPCs

6.2.1 Creating a VPC

Scenarios

A VPC provides an isolated virtual network for your cloud resources. You can configure and manage the network as required. For more information about VPCs, see **Edge Network Overview > VPCs**.

After you create a VPC, you can assign **virtual IP addresses** and **EIPs**, and configure **security groups** and **network ACLs** based on your network requirements.

Constraints and Limitations

- By default, you can use one HUAWEI CLOUD account to create a maximum of 50 edge VPCs. If you want to create more edge VPCs, increase the quota by referring to **Quota Adjustment**.
- By default, subnets in the VPCs are automatically created by the system when you create the edge service. If you need to manually plan the subnets, contact customer service. All subnets mentioned in this chapter are system created.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **VPCs**. On the displayed page, click **Create VPC**.

 Copyright © Huawei Technologies Co., Ltd.

Step 4 On the **Create VPC** page, set required parameters.

Table 6-1 VPC parameter description

Parameter	Description	Example Value
Name	VPC name. The name can contain a maximum of 64 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.	VPC-001
Subnet Planning	The way subnets are created. The default value is **Automatic**. The VPC will not contain subnets after you create it. After you create an edge service, the system automatically generates one or more subnets for the edge service. You can delete the subnets, but you cannot add them.	Automatic
CIDR Block	IP address range for the VPC. The subnets must be within the IP address range of the VPC. The following CIDR blocks are supported: 10.0.0.0/8-16 172.16.0.0/12-16 192.168.0.0/16	192.168.0.0/16

Step 5 Confirm the configuration and click **Create Now**.

----End

6.2.2 Managing VPCs

Viewing a VPC

In the navigation pane on the left, choose **Edge Networks** > **VPCs**. In the VPC list, view the VPC information. You can also click **Create Edge Service** in the **Operation** column to switch to the page for creating an edge service.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-2 VPC information

Parameter	Description
Name/ID	• **Name**: VPC name that you entered during VPC creation. You can click the VPC name to view and manage subnets on the VPC details page. • **ID**: After a VPC is created, the system automatically generates an ID. The ID is globally unique and allows operations on IEC resources through APIs. Click  next to ID to copy it.
CIDR Block	IP address range for the VPC that you specified during VPC creation.
Subnets	Number of subnets in the VPC. A VPC will not contain any subnets after you create it. After you create an edge service, the system automatically generates one or more subnets for the edge service. You can delete the subnets, but you cannot add them.
Subnet Planning	The way subnets are created. The default value is **Automatic**.

Deleting a VPC

You can delete a VPC if it is no longer needed.

Before you delete the VPC, ensure that it does not contain any subnets.

Locate the VPC you want to delete and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

6.2.3 Managing Subnets

Viewing Subnets

In the left navigation pane, choose **Edge Networks** > **VPCs**. On the displayed page, locate the VPC and click its name to view the subnets.

By default, you can use one HUAWEI CLOUD account to create a maximum of 150 subnets. If you want to create more subnets, increase the quota by referring to **Quota Adjustment**.

Copyright © Huawei Technologies Co., Ltd.

Table 6-3 Subnet information

Parameter	Description
Name/ID	• **Name**: subnet name, which is automatically generated by the system after you create a VPC. Click the name of a subnet to go to the subnet details page, change the subnet name, view and change the DNS server IP address, and apply for and view a virtual IP address. • **ID**: Automatically generated by the system. The ID is globally unique and allows operations on IEC resources through APIs.
CIDR Block	IP address range of the subnet, which is automatically assigned by the system upon VPC creation.
Region	Specific location of the edge site for which the subnet created for. The value is generated by the system by default after the VPC is created.
DHCP	By default, the subnet is configured with Dynamic Host Configuration Protocol (DHCP). That is, after the edge instance that uses the subnet is started, the instance automatically obtains the IP address through DHCP.
Route Table	Name of the custom route table associated with the subnet. You can click the name to go to the details page and perform related operations.

Deleting a Subnet

If you no longer require a subnet, you can delete it to release network resources.

Before you delete a subnet, ensure that it does not contain resources such as edge instances, private IP addresses, and virtual IP addresses, and is not associated with a custom route table.

In the subnet list, locate the subnet you want to delete and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

6.3 Route Tables

6.3.1 Creating a Route Table

Scenarios

Create a route table for subnets with the same routing requirements. For details, see **Route Tables**.

The following is the complete process for configuring a route table:

 Copyright © Huawei Technologies Co., Ltd.

1. Create a route table by following the operations provided in this section.
2. Add routes to the route table by referring to **Adding a Route**.
3. Associate one or more subnets with the route table by referring to **Associating a Subnet with a Custom Route Table**.

   After the association is successful, the routes will take effect for the subnets.

Constraints and Limitations

- By default, you can use one HUAWEI CLOUD account to create a maximum of 10 route tables for a VPC. If you need to create more route tables, increase the quota by referring to **Quota Adjustment**.
- A maximum of 200 routes can be added to each route table.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Route Tables**. In the upper right corner, click **Create Route Table**.

Step 4 On the **Create Route Table** page, configure the parameters.

Table 6-4 Route table parameters

Parameter	Description	Example Value
Name	(Mandatory) Route table name. The name can contain a maximum of 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.	rtb-001
VPC	(Mandatory) VPC that the route table belongs to.	vpc-001
Description	(Optional) Supplementary information about the route table. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A
Add Route	(Optional) A button that you can click to add routes to the route table. You can add routes now or after the route table is created. For details, see **Adding a Route**. Each time when you want to add a route, click **+**.	N/A

Step 5 Click **OK**.

Copyright © Huawei Technologies Co., Ltd.

A message is displayed. You can determine whether to associate the route table with subnets immediately. If you want to associate immediately, perform the following operations:

1. Click **Associate Subnet**.
   The **Associated Subnet** page is displayed.
2. Click **Associate Subnet** and select the subnets to be associated.
3. Click **OK**.

----End

6.3.2 Managing Custom Route Tables

Viewing Custom Route Table Information

In the navigation pane on the left, choose **Edge Networks** > **Route Tables**. On the displayed page, locate the route table you want to view.

Table 6-5 Route table information

Parameter	Description
Name	Route table name that you entered during route table creation. You can click the name to go to the details page and view and manage the route table.
VPC	VPC that the route table belongs to.
Type	Only custom route tables are displayed.
Associated Subnets	Number of subnets associated with the route table.

Deleting a Custom Route Table

You can delete only custom route tables.

Before you delete a custom route table, ensure that no subnet is associated with it. If there is an associated subnet, associate the subnet with another route table by clicking **Change Route Table** and then delete the route table.

In the route table list, locate the route table you want to delete and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

6.3.3 Adding a Route

Scenarios

Each route table contains a default system route, which allows that ECSs in a VPC to communicate with each other. You can add custom routes as required to forward the traffic destined for the destination to the specified next hop.

 Copyright © Huawei Technologies Co., Ltd.

For details, see **Routes**.

Constraints and Limitations

When edge instances in a VPC need to access the Internet, you need to add a route and set **Destination** to the default value **0.0.0.0/0** and **Next Hop** to the edge instance or virtual IP address that has an EIP bound in the VPC.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Route Tables**.

Step 4 In the route table list, click the name of the route table that you want to add a route to.

Step 5 Click **Add Route** and set the parameters.

Each time when you want to add a route, click **+**.

Table 6-6 Route parameters

Parameter	Description	Example Value
Destination	Destination CIDR block. The destination can be an IPv4 CIDR block or IPv6 CIDR block. The destination of each route must be unique. The destination cannot overlap with any subnet CIDR block in the VPC.	192.168.0.0/16
Next Hop Type	Type of the next hop. The next hop can be an edge instance or a virtual IP address.	Edge instance
Next Hop	Next-hop resource. The resources in the drop-down list box are displayed based on the selected next hop type.	vm-001
Description	Supplementary information about the route. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

Step 6 Click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

6.3.4 Managing Custom Routes

Viewing a Route

View a route on the route table details page.

Table 6-7 Route information

Parameter	Description
Destination	Destination CIDR block.
Next Hop Type	Type of the next hop.
Next Hop	Next-hop resource.
Type	Route type. A route can be system route (**System**) or a custom route (**Custom**).
Description	Supplementary information about the route.

Modifying a Route

You can modify only custom routes.

In the route list, locate the route you want to modify and click **Modify** in the **Operation** column. In the displayed dialog box, modify the route and click **OK**.

Deleting a Route

You can delete only custom routes.

In the route list, locate the route you want to delete and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

6.3.5 Associating a Subnet with a Custom Route Table

Scenarios

After a subnet is associated with a custom route table, the routes in the route table control the routing for the subnet and apply to all cloud resources in the subnet. Determine the impact on services before performing this operation.

Constraints and Limitations

A subnet can only be associated with one route table.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

 Copyright © Huawei Technologies Co., Ltd.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Route Tables**.

Step 4 In the route table list, locate the route table you want to associate the subnet with and click **Associate Subnet** in the **Operation** column.

Step 5 Select the subnet to be associated.

Step 6 Click **OK**.

Go to the route table details page and view the associated subnet on the **Associated Subnets** tab page.

----End

6.3.6 Disassociating a Subnet from a Custom Route Table

Scenarios

You need to disassociate a subnet from a custom route table if you want to:

Associate a subnet that has been associated with a custom route table with the default route table of a VPC. After you disassociate the subnet from the custom route table, the subnet is automatically associated with the default route table of the VPC.

To change the default route table to a custom route table, see **Associating a Subnet with a Custom Route Table**. To change a custom route table to another one, see **Changing the Custom Route Table Associated with a Subnet**.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Route Tables**.

Step 4 Locate the route table and click its name to go to the details page.

Step 5 Click **Associated Subnets**.

Step 6 Select the subnet you want to disassociate from the custom route table and click **Disassociate Subnet**.

After the route table is changed to the default one, the routes in the default route table will take effect. Confirm the impact on services and exercise caution when performing this operation.

Step 7 Click **OK**.

----End

Copyright © Huawei Technologies Co., Ltd.

6.3.7 Changing the Custom Route Table Associated with a Subnet

Scenarios

Change the custom route table associated with a subnet to another custom route table.

After the route table is changed, routes in the new route table will apply to all resources in the subnet. Determine the impact on services before performing this operation.

Constraints and Limitations

If a subnet has been associated with a custom route table, you cannot change the custom route table to the default route table. You can only change the custom route table to another custom route table.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Route Tables**.

Step 4 In the route table list, click the name of the target route table.

Step 5 Under **Associated Subnets**, locate the subnet, click **Change Route Table** in the **Operation** column, and select a route table.

Step 6 Click **OK**.

After the route table for a subnet is changed, routes in the new route table will apply to all cloud resources in the subnet.

----End

6.4 Bandwidths

6.4.1 Viewing Bandwidth Information

Scenarios

After you assign an EIP, if the carrier line using the EIP does not have a shared bandwidth allocated to it, the system automatically allocates a shared bandwidth to it.

All EIPs using the same carrier line share the same bandwidth. Different carrier lines use different bandwidths. For details about bandwidth, see **Bandwidth Management**.

 Copyright © Huawei Technologies Co., Ltd.

You can view basic information about a bandwidth, including the bandwidth name/ID, size, and number of EIPs. You can also view **monitoring data** of the shared bandwidth on each line.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Bandwidths**.

Step 4 On the **Edge Bandwidths** page, view the bandwidth information.

Table 6-8 Bandwidth parameter description

Parameter	Description
Name/ID	• **Name**: The bandwidth name is automatically generated by the system based on the edge site. You can click the bandwidth name to go to the bandwidth details page and view basic information, EIPs and instances bound, and **bandwidth monitoring data**. • **ID**: Default ID automatically generated by the system. The ID is globally unique and allows operations on IEC resources through APIs.
Size	The bandwidth automatically generated by the system is **300** Mbit/s by default. You can increase the bandwidth based on the actual network requirements of the carrier line at the edge site. For details, see **Modifying a Bandwidth**.
Billing Mode	IEC provides enhanced 95th percentile bandwidth billing by default. For more information, see **BillingBilling**.
EIPs	You can add multiple EIPs to a shared bandwidth at a time. These EIPs are bound to edge instances that are at the same edge site of these EIPs. By default, you can use one HUAWEI CLOUD account to add a maximum of 150 EIPs to a shared bandwidth. If you want to assign more EIPs, increase the quota by referring to **Quota Adjustment**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Status	Bandwidth status. The status can be **In use** or **Frozen**. You cannot use a bandwidth that is in the **Frozen** state because the account is in arrears. If your account is in arrears, top up your HUAWEI CLOUD account. After the top-up, the system will unfreeze the bandwidth in the next required service usage duration. For more information, see **Billing**.
Site	Specific location of the edge site where the shared bandwidth is used
Line	Carrier line that uses the shared bandwidth.

----End

6.4.2 Modifying a Bandwidth

Scenarios

You can modify the name and size of a shared bandwidth as required. Example:

- Change the bandwidth name automatically generated by the system to a name that is easy to identify.

  Bandwidths with the same name can co-exist.
- Increase or decrease the bandwidth based on the network traffic planned for the carrier line at the edge site.

Modifying the Bandwidth on the Edge Bandwidths Page

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Bandwidths**.

Step 4 In the bandwidth list, locate the bandwidth you want to modify and click **Modify** in the **Operation** column.

Step 5 Change the bandwidth name or size.

You can also click  next to the bandwidth name to change the bandwidth name.

Step 6 Click **Finish**.

----End

 Copyright © Huawei Technologies Co., Ltd.

Modifying the Bandwidth on the Bandwidth Details Page

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Bandwidths**.

Step 4 In the bandwidth list, click the name of the target bandwidth.

Step 5 In the upper right corner of the bandwidth details page, click **Modify Bandwidth**.

Step 6 Change the bandwidth name or size.

You can also click next to the bandwidth name in the **Basic Info** area to change the bandwidth name.

Step 7 Click **OK**.

----End

6.4.3 Deleting a Bandwidth

Scenarios

If a bandwidth is no longer needed, you can manually delete it.

Prerequisites

The bandwidth is not used by any EIP.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Bandwidths**.

Step 4 In the bandwidth list, locate the bandwidth you want to delete and click **Delete** in the **Operation** column.

Step 5 Confirm the information and click **Yes**.

----End

6.5 EIPs

 Copyright © Huawei Technologies Co., Ltd.

6.5.1 Assigning an EIP and Binding It to an Edge Instance or Virtual IP Address

Scenarios

You can assign an EIP and bind it to an edge instance or a virtual IP address to enable the edge instance to access the Internet.

Constraints and Limitations

By default, you can use one HUAWEI CLOUD account to assign a maximum of 150 EIPs. If you want to assign more EIPs, increase the quota by referring to **Quota Adjustment**.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **EIPs**.

Step 4 On the **Edge EIPs** page, click **Assign EIP** in the upper right corner.

Step 5 Select the edge location and carrier line that use the EIP.

Step 6 Click **OK**.

Step 7 On the **Edge EIPs** page, locate the EIP, and click **Bind** in the **Operation** column.

Step 8 Select the edge instance (and NIC) or virtual IP address to which you want to bind the EIP.

Step 9 Click **OK**.

----End

6.5.2 Viewing EIP Information

Scenarios

After an EIP is assigned, you can view its information on the **Edge EIPs** page, including its status, bandwidth name and size, and edge instance or virtual IP address to which the EIP is bound.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **EIPs**.

Step 4 View basic information about the EIPs on the **Edge EIPs** page.

Table 6-9 EIP information

Parameter	Description
EIP	Idle IP address automatically assigned to the edge site.
Status	EIP status. The value can be **Unbound** or **Bound**.
EIP for Direct Access	Whether the EIP is used for direct Internet access.
Bandwidth	Name of the bandwidth that the EIP is added to. After you select a carrier line at the edge site when you assign the EIP, the bandwidth is automatically created.
Bandwidth Details	Size of the shared bandwidth that the EIP is added to.
Edge Instance/ Virtual IP Address	Edge instance or virtual IP address to which the EIP is bound.
Region	Specific location of the edge site where the EIP is used.
Line	Carrier line that the EIP uses for network communications.

----End

6.5.3 Unbinding or Releasing an EIP

Unbinding an EIP from an Edge Instance or a Virtual IP Address

If an edge instance or a virtual IP address no longer requires an EIP, you can unbind the EIP from the edge instance or virtual IP address.

1. On the **Edge EIPs** page, locate the EIP, and click **Unbind** in the **Operation** column.
2. Click **OK**.

After unbinding an EIP, you can click **Bind** to bind the EIP to another edge instance or a virtual IP address.

Releasing an EIP

If an edge instance or a virtual IP address no longer requires an EIP, you can release the EIP.

- You can only release EIPs that are not bound to any resources. To release EIPs that are bound, you must first unbind them.
- You cannot use a released EIP if it is currently being used by another user.

 Copyright © Huawei Technologies Co., Ltd.

In the EIP list, locate the EIP you want to release and click **Release** in the **Operation** column.

6.6 Virtual IP Addresses

6.6.1 Assigning a Virtual IP Address

Scenarios

When you need to configure a virtual IP address or reserve a specified virtual IP address for an edge instance, you can assign a virtual IP address for the subnet the edge instance belongs to.

For details about virtual IP addresses, see **Edge Network Overview > Virtual IP Addresses**.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **VPCs**.

Step 4 On the **Edge VPCs** page, locate the VPC containing the subnet to which you want to assign a virtual IP address, and click the VPC name.

Step 5 On the **Subnets** tab, click the name of the subnet that you want to assign a virtual IP address from.

The subnet details page is displayed.

Step 6 Under **Virtual IP Addresses**, click **Assign Virtual IP Address**.

Step 7 Select a virtual IP address assignment mode.

- **Automatic**: The system assigns an IP address automatically.
- **Manual**: You can specify an IP address.

Step 8 (Optional) If you select **Manual**, enter an IP address.

Step 9 Confirm the information and click **OK**.

----End

6.6.2 Managing Virtual IP Addresses

Viewing Virtual IP Address Information

You can view the virtual IP address information on the subnet details page.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-10 Virtual IP address information

Parameter	Description
Virtual IP Address	• Automatically assigned by the system or you specified • **ID**: Automatically generated by the system. The ID is globally unique and allows operations on IEC resources through APIs.
EIP Bound	You can bind an EIP to the virtual IP address.
Server Bound (NIC)	You can access an edge instance through the virtual IP address bound to it.

Deleting a Virtual IP Address

Delete a virtual IP address that you no longer need or a reserved virtual IP address to avoid wasting resources.

Before you delete a virtual IP address, ensure that it has been unbound from the following resources:

- Edge instance
- EIP

In the virtual IP address list, locate the virtual IP address you want to delete and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

6.6.3 Binding a Virtual IP Address to an EIP or Edge Instance

Scenarios

You can bind a virtual IP address to an EIP or edge instance.

Before you bind a virtual IP address to an EIP, ensure that the virtual IP address has been bound to an edge instance so that the virtual IP address can be accessed through the EIP.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **VPCs**.

Step 4 On the **Edge VPCs** page, locate the VPC containing the subnet to which you want to bind a virtual IP address, and click the VPC name.

Step 5 On the **Subnets** tab, click the name of the subnet that you want to bind a virtual IP address to.

 Copyright © Huawei Technologies Co., Ltd.

The subnet details page is displayed.

Step 6 Locate the virtual IP address you want to bind to an EIP or edge instance, and click **Bind to EIP** or **Bind to Edge Instance** in the **Operation** column.

Step 7 Select the target EIP or edge instance and its NIC.

- If an edge instance has multiple NICs, it is recommended that you bind the virtual IP address to the primary NIC.
- You can bind multiple virtual IP addresses to the NIC of an edge instance.

Step 8 Click **OK**.

----End

Follow-up Operations

Manually configuring a virtual IP address for an edge instance that has been bound with the virtual IP address

After a virtual IP address is bound to an edge instance NIC, you need to manually configure the virtual IP address on the edge instance.

Linux edge instance (CentOS 7.2 64bit is used as an example here.)

1. Check the NIC to which you want to bind the virtual IP address and the NIC connection.

   nmcli connection

   Figure 6-4 Checking the NIC and its connection

   ```
   # nmcli connection
   NAME         UUID                                  TYPE      DEVICE
   System eth0  5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  ethernet  eth0
   System eth1  9c92fad9-6ecb-3e6c-eb4d-8a47c6f50c04  ethernet  --
   System eth2  3a73717e-65ab-93e8-b518-24f5af32dc0d  ethernet  --
   System eth3  c5ca0001-6db2-4602-4b46-d771f4330a6d  ethernet  --
   System eth4  84d43311-57c8-8986-f205-9c78cd6ef5d2  ethernet  --
   #
   ```

   In the preceding command output, **eth0** in the **DEVICE** column indicates the NIC the virtual IP address is bound to, and **System eth0** in the **NAME** column indicates the corresponding connection.

2. Modify the corresponding connection and add the virtual IP address.

   nmcli connection modify "*CONNECTION***" ipv4.addresses** *VIP*

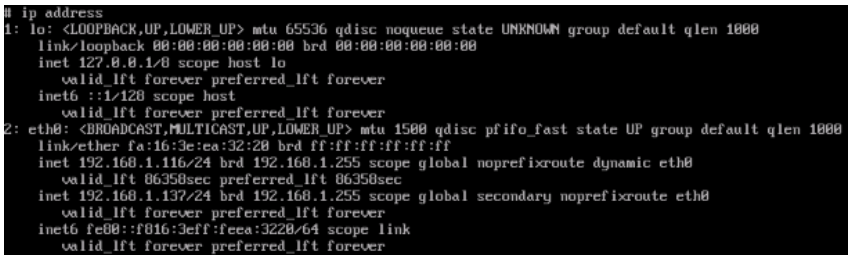
   Figure 6-5 Configuring virtual IP address

   ```
   # nmcli connection modify "System eth0" ipv4.addresses 192.168.1.137/24
   #
   # nmcli connection show "System eth0" | grep -F ipv4.addresses
   ipv4.addresses:                         192.168.1.137/24
   ```

3. Restart the edge instance and run the **ip address** command to check whether the virtual IP address has been configured.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-6 Checking whether the virtual IP address has been configured



In the preceding command output, **192.168.1.137** is the virtual IP address.

Related Operations

What Are the Differences Between EIPs, Private IP Addresses, and Virtual IP Addresses?

6.7 Security Groups

6.7.1 Creating a Security Group

Scenarios

To improve edge instance access security, you can create a security group, and add edge instances in a VPC to the security group. It is good practice to allocate edge instances that have different Internet access policies to different security groups.

By default, a newly created security group does not contain any rules. After you create a security group, you need to **configure security group rules**.

For details about security groups, see **Edge Network Overview > Security Groups**.

Constraints and Limitations

By default, you can use one HUAWEI CLOUD account to create a maximum of 200 edge security groups. If you want to create more security groups, increase the quota by referring to **Quotas**.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Security Groups**.

Step 4 On the **Edge Security Groups** page, click **Create Security Group** in the upper right corner.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Enter a name and description for the security group, and click **OK**.

The name can contain a maximum of 64 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.

The description can contain a maximum of 64 characters and cannot contain angle brackets (< or >).

----End

6.7.2 Managing a Security Group

Viewing Security Group Information

You can view basic information about a security group that you have created, including name, number of rules, number of associated edge instances, and description.

In the navigation pane on the left, choose **Edge Networks** > **Security Groups**. On the displayed page, locate the security group you want to view.

Table 6-11 Security group information

Parameter	Description
Name	Security group name that you entered during creation. Click the name of a security group to view its basic information, inbound and outbound rules, and associated instances.
Rules	Number of configured inbound and outbound rules.
Associated Edge Instances	Number of edge instances that are associated with the security group. When you create an edge service, you can associate it with a specified security group. You can click the number to view details about the associated edge instances.
Description	Supplementary information about the security group.

Deleting a Security Group

- Before you delete a security group, check whether it is used by any edge instance. If it is used by an edge instance, delete the edge instance first and then delete the security group.
- If the security group you want to delete is associated with rules of another security group (**Source Address**), delete or modify the associated security group rules, and then delete the security group.

In the security group list, locate the security group you want to delete and then click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

 Copyright © Huawei Technologies Co., Ltd.

6.7.3 Configuring Security Group Rules

Scenarios

After you create a security group, you can add rules to it. A rule applies either to inbound traffic or outbound traffic. After you add edge instances to the security group, the group's rules apply to the instances.

- Inbound rules control traffic to edge instances in the security group.
- Outbound rules control traffic from edge instances in the security group.

For details about the configuration examples of the security group rule, see **Security Group Configuration Examples**.

Constraints and Limitations

- Edge instances in different VPCs cannot communicate with each other even if these edge instances are associated with the same security group and inbound and outbound rules have been configured for the security group.
- Edge instances on subnets of different edge sites cannot communicate with each other even if inbound and outbound security group rules have been configured for the edge instances.
- By default, you can use one HUAWEI CLOUD account to create a maximum of 10,000 security group rules. If you want to configure more security group rules, increase the quota by referring to **Quota Adjustment**.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Security Groups**.

Step 4 On the **Edge Security Groups** page, locate the security group, click **Configure Rule** in the **Operation** column or click the security group name in the **Name** column to view the security group details.

Step 5 Under **Inbound Rules**, click **Add**. In the displayed **Add Inbound Rule** dialog box, set the parameters.

- Click **+** to add more inbound rules.
- Click **Copy** at the end of a rule and modify the copied rule as required to quickly generate a new one.

Copyright © Huawei Technologies Co., Ltd.

Table 6-12 Inbound rule parameter description

Parameter	Description	Example Value
Priority	Priority of the security group rule. The priority value ranges from 1 to 100. The default priority is 1 and has the highest priority. The rule with a smaller value has a higher priority.	1
Action	Action of the security group rule. Deny rules take precedence over allow rules if the rules have the same priority.	Allow
Protocol & Port	Network protocol. Possible values are **All**, **TCP**, **UDP**, **ICMP**, and **GRE**.	TCP
	Port: Port or port range over which traffic can reach your edge instance. The port ranges from 1 to 65535. For details, see **Common Ports Used by Edge Instances**. Enter ports in the following format: • Individual port: Enter a port, such as **22**. • Consecutive ports: Enter a port range, such as **22-30**. • All ports: Leave it blank or enter **1-65535**.	22, or 22-30, or 20,22-30
Source	**Source**: Source of the security group rule. The value can be a single IP address or another edge security group. Example: • xxx.xxx.xxx.xxx/32 (IPv4 address) • xxx.xxx.xxx.0/24 (subnet) • 0.0.0.0/0 (any IP address)	0.0.0.0/0
Description	(Optional) Supplementary information about the security group rule. The description can contain a maximum of 64 characters and cannot contain angle brackets (< or >).	N/A

Step 6 Under **Outbound Rules**, click **Add**. In the displayed **Add Outbound Rule** dialog box, set the parameters.

- Click **+** to add more outbound rules.
- Click **Copy** at the end of a rule and modify the copied rule as required to quickly generate a new one.

Copyright © Huawei Technologies Co., Ltd.

Table 6-13 Outbound rule parameter description

Parameter	Description	Example Value
Priority	Priority of the security group rule. The priority value ranges from 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	Action of the security group rule. Deny rules take precedence over allow rules if the rules have the same priority.	Allow
Protocol & Port	Network protocol. Possible values are **All**, **TCP**, **UDP**, **ICMP**, and **GRE**.	TCP
	Port: Port or port range over which traffic can leave your edge instance. The port ranges from 1 to 65535. For details, see **Common Ports Used by Edge Instances**. Enter ports in the following format: – Individual port: Enter a port, such as **22**. – Consecutive ports: Enter a port range, such as **22-30**. – All ports: Leave it blank or enter **1-65535**.	22, or 22-30, or 20,22-30
Destination	**Destination**: Destination of the security group rule. The value can be a single IP address or another edge security group. Example: – xxx.xxx.xxx.xxx/32 (IPv4 address) – xxx.xxx.xxx.0/24 (subnet) – 0.0.0.0/0 (any IP address)	0.0.0.0/0
Description	(Optional) Supplementary information about the security group rule. The description can contain a maximum of 64 characters and cannot contain angle brackets (< or >).	N/A

Step 7 Click **OK**.

----End

Verifying Configurations

After you add the security group rules, check whether the rules have taken effect. Assume that you deploy a website on an edge instance and add the following inbound rule to allow TCP traffic over port 80.

Copyright © Huawei Technologies Co., Ltd.

Table 6-14 Security group rule

Direction	Priority	Action	Protocol	Port/Range	Source
Inbound	1	Allow	TCP	80	0.0.0.0/0

To verify the security group rule on a Linux edge instance:

Step 1 Log in to an edge instance.

Step 2 Check whether TCP port 80 is listened.

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

Step 3 If command output shown in **Figure 6-7** is displayed, TCP port 80 is listened.

Figure 6-7 Command output for the Linux edge instance



Step 4 In the address box of the browser, enter **http://***EIP bound to the edge instance* and press **Enter**.

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

----End

6.7.4 Managing Security Group Rules

Viewing Security Group Rules

After you add a security group rule, you can view its basic information, such as the protocol, and port.

In the left navigation pane, choose **Edge Networks** > **Security Groups** and click the security group name to go to the details page and view the configured inbound and outbound rules.

Table 6-15 Security group rule information

Parameter	Description
Priority	Priority of the security group rule. The priority value ranges from 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.
Action	Action of the security group rule. Deny rules take precedence over allow rules if the rules have the same priority.
Protocol	Network protocol. Possible values are **All**, **TCP**, **UDP**, **ICMP**, and **GRE**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Port/Range	• Inbound: Port or port range over which the traffic can reach your edge instance. The port ranges from 1 to 65535. • Outbound: Port or port range over which traffic can leave your edge instance. The port ranges from 1 to 65535.
Source/ Destination	Source or destination IP address you configured when adding a security group rule.
Description	Supplementary information about the security group rule.

Deleting a Security Group Rule

If the source of an inbound security group rule or destination of an outbound security group rule needs to be changed, you need to first delete the security group rule and add a new one.

On the **Edge Security Groups** page, locate the security group, click **Configure Rule** in the **Operation** column or click the security group name in the **Name** column to view the security group details.

On the **Inbound Rules** or **Outbound Rules** tab, locate the row that contains the target rule and click **Delete** in the **Operation** column.

You can also select multiple security group rules and click **Delete** above the security group rule list to delete multiple rules at once.

6.7.5 Importing or Exporting Security Group Rules

Scenarios

- If you want to quickly create or restore a security group rule, you can import the exported security group rule file to the security group.
- If you want to back up security group rules locally, you can export the security group rules to an Excel file.
- If you want to quickly apply the rules of a security group to another, or batch modify the rules of the current security group, you can import or export existing rules.

Constraints and Limitations

- When modifying exported security group rules, you can only modify existing fields in the exported file based on the template and cannot add new fields or modify the field names. Otherwise, the exported file cannot be imported into the system.
- If there are duplicate security group rules, only duplicate rules cannot be imported.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Security Groups**.

Step 4 On the **Edge Security Groups** page, click the security group name.

Step 5 On the displayed page, export or import security group rules.

- Click  to export all rules of the current security group to an Excel file.
- Click  to import security group rules from an Excel file into the current security group.

----End

6.7.6 Changing a Security Group

Scenarios

Change the security group to which the NIC of an edge instance belongs as required.

Procedure

Step 1 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

Step 2 The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Instances**.

Step 4 In the edge instance list, locate the edge instance whose security group you want to change, click **More** in the **Operation** column, and select **Change Security Group**.

Step 5 Select the target NIC and security group as prompted.

Step 6 Click **Yes**.

- You can select a maximum of five security groups. Using multiple security groups may affect the network performance of edge instances.
- To create a security group, click **Create Security Group**.
- You can go to the edge instance details page and change the security group on the **NICs** or **Security Groups** tab page.

----End

 Copyright © Huawei Technologies Co., Ltd.

6.7.7 Security Group Configuration Examples

This section shows common security group configuration examples. The following examples allow all outgoing data packets by default and only describe how to configure the inbound rules of a security group.

- **Allowing External Access to a Specified Port**
- **Enabling Edge Instances In Different Security Groups to Communicate Through an Internal Network**
- **Enabling Specified IP Addresses to Remotely Access Edge Instances in a Security Group**
- **Enabling Remote SSH Access to Linux Edge Instances**
- **Pinging the Edge Instance from the Internet**
- **Using the Edge Instance as a Web Server**
- **Using the Edge Instance as a DNS Server**
- **Uploading or Downloading Files Using FTP**

You need to create a security group in advance. For details, see **Creating a Security Group** and **Configuring Security Group Rules**.

For details, see **Common Ports Used by Edge Instances**.

Allowing External Access to a Specified Port

- Example scenario

  After you deploy services, you can add security group rules to allow external access to a specified port (for example, port 1100).

- Security group configuration

Direction	Priority	Action	Protocol	Port/ Range	Source
Inbound	1	Allow	TCP	1100	0.0.0.0/0

Enabling Edge Instances In Different Security Groups to Communicate Through an Internal Network

- Example scenario

  In the same VPC at the same edge site, if you need to copy resources from an edge instance in a security group to an edge instance in another security group, you can configure the two edge instances so that they can communicate with each other through a private network and then copy the resources.

- Security group configuration

  By default, edge instances in the same security group of the same VPC at the same edge site can communicate with each other, whereas edge instances in different security groups cannot. To enable these edge instances to communicate with each other, add security group rules.

  You can add an inbound rule to the security groups containing the edge instances to allow access from edge instances in the other security group.

 Copyright © Huawei Technologies Co., Ltd.

Direction	Priority	Action	Protocol	Port/Range	Source
Inbound	Priority of a rule	Select **Allow** or **Deny**.	Protocol used for communications over a private network	Port or port range	Name of the other security group

Enabling Specified IP Addresses to Remotely Access Edge Instances in a Security Group

- Example scenario

  To prevent attacks on edge instances, you can change the port number for remote login and configure security group rules that allow only specified IP addresses to remotely access the edge instances.

- Security group configuration

  To allow IP address 192.168.20.2 to remotely access Linux edge instances in a security group over SSH and port 22, configure the following security group rule.

Direction	Priority	Action	Protocol	Port/Range	Source
Inbound	1	Allow	SSH (22)	22	IPv4 CIDR block or ID of another security group For example, 192.168.20.2/32

Enabling Remote SSH Access to Linux Edge Instances

- Example scenario

  After you create a Linux edge instance, add a security group rule to enable remote SSH access to the edge instance.

- Security group configuration

Direction	Priority	Action	Protocol	Port/Range	Source
Inbound	1	Allow	SSH (22)	22	0.0.0.0/0

Pinging the Edge Instance from the Internet

- Example scenario

  After you create edge instances, add a security group rule so that you can run the **ping** command to test communication between the edge instances.

Copyright © Huawei Technologies Co., Ltd.

- Security group configuration

Direction	Priority	Action	Protocol	Port/Range	Source
Inbound	1	Allow	ICMP	All	0.0.0.0/0

Using the Edge Instance as a Web Server

- Example scenario

  If you have deployed a website on your edge instance and want to allow access to your website over HTTP or HTTPS, you need to add rules to the security group containing the edge instance.

- Security group configuration

Direction	Priority	Action	Protocol	Port/ Range	Source
Inbound	1	Allow	HTTP (80)	80	0.0.0.0/0
Inbound	1	Allow	HTTPS (443)	443	0.0.0.0/0

Using the Edge Instance as a DNS Server

- Example scenario:

  If you use an edge instance as a DNS server, add security group rules to allow TCP and UDP traffic to the edge instance over port 53. Add the following rules to the security group.

- Security group configuration

Direction	Priority	Action	Protocol	Port/ Range	Source
Inbound	1	Allow	TCP	53	0.0.0.0/0
Inbound	1	Allow	UDP	53	0.0.0.0/0

Uploading or Downloading Files Using FTP

- Example scenario

  If you want to use FTP to upload files to or download files from an edge instance, add the following security group rule.

  NOTE

  You need to install the FTP server program on the edge instance and check whether port 20 and 21 work properly.

- Security group configuration

 Copyright © Huawei Technologies Co., Ltd.

Direction	Priority	Action	Protocol	Port/ Range	Source
Inbound	1	Allow	TCP	20-21	0.0.0.0/0

6.7.8 Commonly Used Ports

Table 6-16 lists the common ports used by edge instances. You can configure security group rules to allow traffic to and from the ports of these edge instances. For details, see **Configuring Security Group Rules**.

Table 6-16 Commonly-used ports

Protocol	Port	Description
FTP	21	A port used to upload and download files
SSH	22	A port used to remotely access the edge instances
Telnet	23	A port used to remotely log in to the edge instances over Telnet
HTTP	80	A port used to access websites over HTTP
POP3	110	A port used to receive emails using Post Office Protocol version 3 (POP3)
IMAP	143	A port used to receive emails using Internet Message Access Protocol (IMAP)
HTTPS	443	A port used to access websites over HTTPS
RDS for SQL Server	1433	A TCP port of the RDS for SQL Server for providing services
RDS for SQL Server	1434	A UDP port of the RDS for SQL Server for returning the TCP/IP port number used by the RDS for SQL Server
Oracle	1521	Oracle database communications port, which must be enabled on the edge instances where Oracle SQL Server is deployed
RDS for MySQL	3306	A port used by RDS for MySQL databases to provide services
Proxy	8080	A proxy port used in the WWW proxy service for web browsing. If you use port 8080, you need to add **:8080** after the IP address when you visit a website or use a proxy server. If you install Apache Tomcat, the default service port is 8080.

Copyright © Huawei Technologies Co., Ltd.

Protocol	Port	Description
NetBIOS	137, 138, 139	NetBIOS is often used for Windows files, printer sharing, and Samba. • Ports 137 and 138: UDP ports that are used when transferring files using Network Neighborhood (My Network Places) • Port 139: Connections from this port try to access the NetBIOS/SMB service.

Some ports are inaccessible.

Symptom: Users in some areas cannot access some ports in the public cloud system.

Analysis: Ports listed in the following table are high-risk ports and are blocked by default.

Table 6-17 High-risk ports

Protocol	Port
TCP	42 135 137 138 139 444 445 593 1025 1068 1434 3127 3128 3129 3130 4444 5554 5800 5900 9995 9996
UDP	135~139 1026 1027 1028 1068 1433 1434 5554 9995 9996

Solution: Do not use ports listed in the preceding table for your services.

6.8 Network ACLs

6.8.1 Creating a Network ACL

Scenarios

A network ACL is an optional layer of security for your subnets. You associate one or more subnets with a network ACL. The network ACL can help control traffic in and out of the subnets. Your VPC does not have a network ACL by default. If needed, you can create a network ACL and associate it with subnets. For details about network ACLs, see **Edge Network Overview > Network ACLs**.

The following process shows how to use a network ACL:

1. **Create a network ACL**.
2. **Configure a network ACL** or use the default rule.
3. **Associate a network ACL with subnets**. After the association, the subnets will be protected by the configured network ACL rules.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Network ACLs**.

Step 4 On the **Edge Network ACLs** page, click **Create Network ACL** in the upper right corner.

Step 5 Enter a name and description for the network ACL, and click **OK**.

The name can contain a maximum of 64 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.

The description can contain a maximum of 64 characters and cannot contain angle brackets (< or >).

----End

6.8.2 Managing Network ACLs

Viewing Network ACLs

In the navigation pane on the left, choose **Edge Networks** > **Network ACLs**. On the displayed page, locate the network ACL you want to view.

Table 6-18 Network ACL information

Parameter	Description
Name	Network ACL name. Click the name of a network ACL to view its basic information, inbound and outbound rules, and associated edge subnets.
Status	Network ACL status, which can be **Enabled** or **Disabled**.
Network ACL Rules	Number of inbound and outbound rules configured for the network ACL.
Description	Supplementary information about the network ACL.

Modifying a Network ACL

If needed, you can modify the name and description of a network ACL.

Click the network ACL name to go to the details page, and click  next to the name or description to modify it. Click √ to save the modification.

 Copyright © Huawei Technologies Co., Ltd.

Enabling or Disabling a Network ACL

- After you create a network ACL, you can enable or disable it based on your network security requirements. Before enabling a network ACL, ensure that subnets have been associated with the network ACL and that inbound and outbound rules have been added to the network ACL.
- When a network ACL is disabled, custom rules will become invalid. However, default network ACL rules will still apply. Disabling a network ACL may interrupt network traffic. For details about the default network ACL rules, see **Default Network ACL Rules**.

On the **Network ACLs** page, locate the network ACL you want to enable or disable, click **More** in the **Operation** column, and select **Enable** or **Disable**.

Deleting a Network ACL

If needed, you can delete a network ACL at any time.

Before you delete a network ACL, check whether it is associated with any subnets. If it is associated with a subnet, disassociate it from the subnet and then delete it.

After a network ACL is deleted, the rules added to the network ACL are also deleted.

On the **Network ACLs** page, locate the network ACL you want to delete, click **More** in the **Operation** column, and select **Delete**. In the displayed dialog box, click **Yes**.

6.8.3 Configuring a Network ACL

Scenarios

You can add inbound and outbound rules to the network ACLs you create. A rule applies either to inbound traffic or outbound traffic. The subnet associated with a network ACL is protected by the network ACL rules.

- Inbound: allows traffic from the Internet to the subnets associated with the network ACL
- Outbound rule: allows subnets associated with the network ACL rule to access subnets not associated with the network ACL.

For details about the configuration examples of the network ACL rule, see **Network ACL Configuration Examples**.

Constraints and Limitations

- By default, each network ACL has preset rules that allow the following packets:
  - Packets whose source and destination are in the same subnet and at the same site
  - Broadcast packets with the destination 255.255.255.255/32 that is used for configuring host startup information
  - Multicast packets with the destination 224.0.0.0/24 that is used by routing protocols

Copyright © Huawei Technologies Co., Ltd.

  - Metadata packets with the destination 169.254.169.254/32 and TCP port 80 that are used for obtaining metadata
  - Packets from CIDR blocks that are reserved for public services, for example, packets with the destination 100.125.0.0/16
  - A network ACL denies all traffic in and out of a subnet excepting the preceding ones. **Table 6-19** shows the default network ACL rules. The default rules cannot be modified or deleted.

    Table 6-19 Default network ACL rules

Direction	Priority	Action	Protocol	Source	Destination IP Address	Description
Inbound	*	Deny	All	0.0.0.0/0	0.0.0.0/0	Denies all inbound traffic.
Outbound	*	Deny	All	0.0.0.0/0	0.0.0.0/0	Denies all outbound traffic.

- Network connectivity
  - Edge instances on subnets of different VPCs cannot communicate with each other even if the subnets have the same network ACL and inbound and outbound rules have been configured for the subnets.
  - Edge instances on the subnets of different edge sites cannot communicate with each other even if inbound and outbound network ACL rules have been configured for the edge instances.
- Rule Priorities
  - Network ACL rules have priorities. A smaller priority value indicates a higher priority and the network ACL rule is applied first. The rule whose priority value is an asterisk (*) has the lowest priority.
  - If network ACL rules conflict, the rules with higher priorities take precedence. If you need a rule to take effect before or after a specific rule, you can insert that rule before or after the specific rule.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Network ACLs**.

 Copyright © Huawei Technologies Co., Ltd.

Step 4 On the **Edge Network ACLs** page, locate the network ACL, click **Configure Rule** in the **Operation** column or click the network ACL name in the **Name** column to go to the network ACL details page.

Step 5 Under **Inbound Rules** or **Outbound Rules**, click **Add Rule** to add an inbound or outbound rule.

You can click **+** to add more rules.

Table 6-20 Description

Parameter	Description	Example Value
Action	(Mandatory) Network ACL policy. Currently, the value can be **Allow** or **Deny**.	Allow
Protocol	Protocol supported by the network ACL. This parameter is mandatory. Currently, only **TCP**, **UDP**, **ICMP**, and **All protocols** are available. If you select **All protocols** or **ICMP**, you cannot specify the ports.	TCP
Source	Source IP address that the traffic is allowed from. The default value is **0.0.0.0/0**, which indicates that traffic to all IP addresses is allowed. Example: xxx.xxx.xxx.xxx/32 (IPv4 address) xxx.xxx.xxx.0/24 (subnet) 0.0.0.0/0 (any IP address)	0.0.0.0/0
Source Port Range	Source port or port range. The port ranges from 1 to 65535. For a port range, enter two port numbers connected by a hyphen (-), for example, **1-100**. You must specify this parameter if **TCP** or **UDP** is selected for **Protocol**.	22 or 22-30
Destination	Destination IP address that the traffic is allowed to. The default value is **0.0.0.0/0**, which indicates that traffic to all IP addresses is allowed. Example: xxx.xxx.xxx.xxx/32 (IPv4 address) xxx.xxx.xxx.0/24 (subnet) 0.0.0.0/0 (any IP address)	0.0.0.0/0

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Destination Port Range	Destination port or port range. The port ranges from 1 to 65535. For a port range, enter two port numbers connected by a hyphen (-), for example, **1-100**. You must specify this parameter if **TCP** or **UDP** is selected for **Protocol**.	22 or 22-30
Description	(Optional) Supplementary information about the network ACL rule. The description can contain a maximum of 64 characters and cannot contain angle brackets (< or >).	N/A

Step 6 Click **OK**.

----End

6.8.4 Managing Network ACL Rules

Viewing Network ACL Rules

After you add a network ACL rule, you can view its basic information, including the priority, status, policy, and protocol.

In the left navigation pane, choose **Edge Networks** > **Network ACLs** and click the network ACL name to go to the details page and view the configured inbound and outbound rules.

Table 6-21 Network ACL rule information

Parameter	Description
Priority	Network ACL rules have priorities. A smaller priority value indicates a higher priority and the network ACL rule is applied first. The rule whose priority value is an asterisk (*) has the lowest priority.
Status	Status of the network ACL rule, which can be **Enabled** or **Disabled**.
Action	Network ACL rule policy. The value can be **Allow** or **Deny**.
Protocol	Protocol supported by the network ACL. Currently, only **TCP**, **UDP**, **ICMP**, and **All protocols** are available.
Source	Source IP address that the traffic is allowed from. The default value is **0.0.0.0/0**, which indicates that traffic to all IP addresses is allowed.
Source Port Range	Source port or port range. The port ranges from 1 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Destination	Destination IP address that the traffic is allowed to. The default value is **0.0.0.0/0**, which indicates that traffic to all IP addresses is allowed.
Destination Port Range	Destination port or port range. The port ranges from 1 to 65535.
Description	Supplementary information about the network ACL rule.

Modifying a Network ACL Rule

Modify an inbound or outbound network ACL rule based on your network security requirements.

On the **Edge Network ACLs** page, locate the network ACL, click **Configure Rule** in the **Operation** column or click the network ACL name in the **Name** column to go to the network ACL details page.

On the **Inbound Rules** or **Outbound Rules** tab, locate the rule you want to modify and click **Modify** in the **Operation** column.

Enabling or Disabling a Network ACL Rule

Enable or disable an inbound or outbound network ACL rule based on your network security requirements.

On the **Edge Network ACLs** page, locate the network ACL, click **Configure Rule** in the **Operation** column or click the network ACL name in the **Name** column to go to the network ACL details page.

On the **Inbound Rules** or **Outbound Rules** tab, locate the rule you want to enable or disable, click **More** > in the **Operation** column, and select **Enable** or **Disable**.

Deleting a Network ACL Rule

Delete an inbound or outbound network ACL rule based on your network security requirements.

On the **Edge Network ACLs** page, locate the network ACL, click **Configure Rule** in the **Operation** column or click the network ACL name in the **Name** column to go to the network ACL details page.

On the **Inbound Rules** or **Outbound Rules** tab, locate the row that contains the target rule and click **Delete** in the **Operation** column.

6.8.5 Importing or Exporting Network ACL Rules

Scenarios

You can export inbound and outbound rules of a network ACL as an Excel file, and then import these rules for another network ACL.

 Copyright © Huawei Technologies Co., Ltd.

It is recommended that you import no more than 40 rules each time. Importing rules will not delete existing rules.

Constraints and Limitations

Duplicated rules are not allowed.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Network ACLs**.

Step 4 On the **Edge Network ACLs** page, locate the security group and click its name.

Step 5 Export or import network ACL rules.

- Click  to export the inbound and outbound network ACL rules. The exported rules are stored in an Excel file. You need to download the file to a local directory.
- Click , select the exported Excel file, and click **Import**.

----End

6.8.6 Network ACL Configuration Examples

This section shows common network ACL configuration examples.

- **Denying Access from a Specific Port**
- **Allowing Access from Specific Ports and Protocols**

Denying Access from a Specific Port

You might want to block TCP 445 to protect against the WannaCry ransomware attacks. You can add a network ACL rule to deny all incoming traffic from TCP port 445.

Network ACL configuration

Table 6-22 lists the inbound rule required.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-22 Network ACL rules

Direction	Action	Protocol	Source	Source Port Range	Destination IP Address	Destination Port	Description
Inbound	Deny	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	445	Denies inbound traffic from any IP address through TCP port 445.

Allowing Access from Specific Ports and Protocols

In this example, an edge instance in a subnet is used as the web server, and you need to allow inbound traffic from HTTP port 80 and HTTPS port 443 and allow all outbound traffic regardless of the port. You need to configure both the network ACL rules and security group rules to allow the traffic.

Network ACL configuration

Table 6-23 lists the inbound and outbound network ACL rules required.

Table 6-23 Network ACL rules

Direction	Action	Protocol	Source	Source Port Range	Destination	Destination Port	Description
Inbound	Allow	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	80	Allows inbound HTTP traffic from any IP address to the edge instance in the subnet through port 80.
Inbound	Allow	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	443	Allows inbound HTTPS traffic from any IP address to the edge instance in the subnet through port 443.
Outbound	Allow	All	0.0.0.0/0	All	0.0.0.0/0	All	Allow all outbound traffic from the subnet.

Security group configuration

Table 6-24 lists the inbound and outbound security group rules required.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-24 Security group rules

Direction	Protocol / Application	Port	Source/ Destination	Description
Inbound	TCP	80	Source: 0.0.0.0/0	Allows inbound HTTP traffic from any IP address to edge instances in the security group through port 80.
Inbound	TCP	443	Source: 0.0.0.0/0	Allows inbound HTTPS traffic from any IP address to edge instances in the security group through port 443.
Outbound	All	All	Destination: 0.0.0.0/0	Allow all outbound traffic from the security group.

A network ACL adds an additional layer of security. Even if the security group rules allow more traffic than that actually required, the network ACL rules allow only access from HTTP port 80 and HTTPS port 443 and deny other inbound traffic.

6.8.7 Associating a Network ACL with Subnets

Scenarios

Your network ACL takes effect only after you associate it with a subnet. After the association, the network ACL denies all traffic to and from the subnet by default until you add rules to allow traffic.

Constraints and Limitations

You can associate a network ACL with multiple subnets. However, a subnet can only be associated with one network ACL at a time.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Network ACLs**.

Step 4 On the **Edge Network ACLs** page, locate the network ACL, click **Associate Subnet** in the **Operation** column or click the network ACL name in the **Name** column to go to the network ACL details page.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 On the displayed page, click the **Associated Subnets** tab.

Step 6 Click **Associate**.

Step 7 In the displayed **Associate Subnet** dialog box, select the subnets to be associated with the network ACL, and click **OK**.

----End

6.8.8 Disassociating a Network ACL from a Subnet

Scenarios

Disassociate a subnet from a network ACL when necessary. After the disassociation, you can still associate other network ACLs with the subnet.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Network ACLs**.

Step 4 On the **Edge Network ACLs** page, locate the network ACL, click **Associate Subnet** in the **Operation** column or click the network ACL name in the **Name** column to go to the network ACL details page.

Step 5 On the displayed page, click the **Associated Subnets** tab.

Step 6 Under **Associated Subnets**, locate the network ACL and click **Disassociate** in the **Operation** column.

To disassociate multiple subnets from the network ACL, select multiple subnets and click **Disassociate** in the upper left corner of the subnet list.

Step 7 Click **Yes**.

----End

6.8.9 Changing the Priority of a Network ACL Rule

Scenarios

If network ACL rules conflict, the rules with higher priorities take precedence. If you need a rule to take effect before or after a specific rule, you can insert that rule before or after the specific rule.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

 Copyright © Huawei Technologies Co., Ltd.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **Network ACLs**.

Step 4 On the **Edge Network ACLs** page, locate the network ACL, click **Configure Rule** in the **Operation** column or click the network ACL name in the **Name** column to go to the network ACL details page.

Step 5 Under **Inbound Rules** or **Outbound Rules**, locate the rule, click **More** in the **Operation** column, and select **Insert Rule Above** or **Insert Rule Below**.

Step 6 In the displayed dialog box, configure required **parameters** and click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

7 Monitoring

7.1 Viewing Edge Instance Monitoring Data

Scenarios

Monitoring is an important way to ensure edge instance reliability, availability, and performance. On the IEC console, you can view the performance metrics of your edge instances to learn about their running status.

Prerequisites

The edge instance has been properly running for at least 10 minutes.

Metrics of an edge instance in the **Stopped** or **Faulty** state cannot be viewed. Only after the edge instance is restarted or goes back to normal, you can view its metrics.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Instances**.

The edge instance list is displayed.

Step 4 Select an edge instance and click its name to view its details.

The edge instance details page is displayed.

Step 5 Click the **Monitoring** tab to view the monitoring data.

Step 6 In the monitoring area, view monitoring data by selecting the required time period.

 Copyright © Huawei Technologies Co., Ltd.

For details about the metrics, see **Server Metrics**.

----End

7.2 Metrics

Description

This section describes the namespace, metrics, and dimension of edge instances. You can query these metrics by calling IEC APIs or on the IEC console.

Namespace

SYS.ECS

Metrics

Metric	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
cpu_util	CPU Usage	CPU usage of an edge instance Unit: Percent Formula: CPU usage of an edge instance/ Number of vCPUs in the edge instance	≥ 0%	Edge instance	5 minutes
disk_read_bytes_rate	Disk Read Bandwidth	Number of bytes read from an edge instance disk per second Unit: byte/s Formula: Total number of bytes read from an edge instance disk/ Monitoring interval byte_out = (rd_bytes - last_rd_bytes)/ Time difference	≥ 0 bytes/s	Edge instance	5 minutes

 Copyright © Huawei Technologies Co., Ltd.

Metric	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
disk_read_requests_rate	Disk Read IOPS	Number of read requests sent to the edge instance disk per second Unit: Request/s Formula: Total number of read requests sent to an edge instance disk/ Monitoring interval req_out = (rd_req - last_rd_req)/ Time difference	≥ 0 requests/s	Edge instance	5 minutes
disk_write_requests_rate	Disk Write IOPS	Number of write requests sent to the edge instance disk per second Unit: Request/s Formula: Total number of write requests sent to an edge instance disk/ Monitoring interval req_in = (wr_req - last_wr_req)/ Time difference	≥ 0 requests/s	Edge instance	5 minutes

 Copyright © Huawei Technologies Co., Ltd.

Metric	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
network_incoming_bytes_aggregate_rate	Outband Incoming Rate	Number of incoming bytes on an edge instance per second on the hypervisor Unit: byte/s Formula: Total number of outband incoming bytes on an edge instance/ Monitoring interval	≥ 0 bytes/s	Edge instance	5 minutes
network_outgoing_bytes_aggregate_rate	Outband Outgoing Rate	Number of outgoing bytes on an edge instance per second on the hypervisor Unit: byte/s Formula: Total number of outband outgoing bytes on an edge instance/ Monitoring interval	≥ 0 bytes/s	Edge instance	5 minutes

Dimension

Key	Value
instance_id	Instance ID

7.3 Viewing Bandwidth and EIP Monitoring Data

Viewing Bandwidth Monitoring Data on the Overview Page

Step 1 Log in to the management console.

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 View the trend of the total bandwidth usage.

You can view the trend of outbound and inbound bandwidth changes at all sites.

Step 4 In the **Site Overview** are, view the weekly outbound bandwidth usage peak of each edge site.

Weekly outbound bandwidth usage peak = Peak outbound bandwidth used last week/Bandwidth set for the edge site

----End

Viewing Bandwidth Statistics

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 View the bandwidth statistics.

You can view the daily outbound peak bandwidth, daily inbound peak bandwidth, weekly outbound peak bandwidth peaks, and weekly inbound peak bandwidth of the top 5 IEC sites sorted in descending order.

----End

Viewing the EIP Monitoring Data on the Edge EIPs Page

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Edge Networks** > **EIPs**.

The **Edge EIPs** page is displayed.

Step 4 In the EIP list, locate the EIP whose monitoring data you want to view and click its name.

Step 5 In the monitoring area, view monitoring data by selecting the required time period.

For details about the metrics, see **bandwidth metrics**.

----End

 Copyright © Huawei Technologies Co., Ltd.

7.4 Bandwidth and EIP Metrics

Description

This section describes the namespace, metrics, and dimensions of bandwidth and EIPs. You can query these metrics by calling IEC APIs or on the IEC console.

Namespace

SYS.VPC

Metrics

Metric	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
upstream_bandwidth	Outbound Bandwidth	Network rate of outbound traffic (Previously called "Upstream Bandwidth") Unit: bit/s	≥ 0 bits/s	Bandwidth or EIP	1 minute
downstream_bandwidth	Inbound Bandwidth	Network rate of inbound traffic (Previously called "Downstream Bandwidth") Unit: bit/s	≥ 0 bits/s	Bandwidth or EIP	1 minute
up_stream	Outbound Traffic	Network traffic going out of the cloud platform (Previously called "Upstream Traffic") Unit: byte	≥ 0 bytes	Bandwidth or EIP	1 minute

 Copyright © Huawei Technologies Co., Ltd.

Metric	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
down_stream	Inbound Traffic	Network traffic going into the cloud platform (originally named "Downstream Traffic") Unit: byte	≥ 0 bytes	Bandwidth or EIP	1 minute
upstream_bandwidth_usage	Outbound Bandwidth Usage	Usage of outbound bandwidth in the unit of percent	0-100%	Bandwidth or EIP	1 minute

Dimensions

Key	Value
publicip_id	EIP IDs
bandwidth_id	Bandwidth IDs

If a monitored object has multiple dimensions, specify all dimensions when you use an API to query metrics.

- Query a metric: dim.0=bandwidth_id, 530cd6b0-86d7-4818-837f-935f6a27414d&dim.1=publicip_id, 3773b058-5b4f-4366-9035-9bbd9964714a
- Query metrics in batches from both of the following dimensions:
  "dimensions": [
  {
  "name": "bandwidth_id",
  "value": "530cd6b0-86d7-4818-837f-935f6a27414d"
  }
  {
  "name": "publicip_id",
  "value": "3773b058-5b4f-4366-9035-9bbd9964714a"
  }
  ],

 Copyright © Huawei Technologies Co., Ltd.

8 Alarm

8.1 Creating an Alarm Rule

Scenarios

You can set alarm rules for monitoring metrics. When the monitoring metrics trigger the preset alarm conditions, IEC notifies you by email or SMS message. In this way, you can handle faults in a timely manner to prevent business loss caused by resource problems.

IEC allows you to customize alarm rules only for bandwidth metrics.

Procedure

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**. On the displayed page, click **Create Alarm Rule**.

Step 4 On the **Create Alarm Rule** page, set the parameters.

1. Set the alarm rule name and description.

   Name: Enter a name for the alarm rule. If you do not enter a name, the system generates a random one that you can modify.

   (Optional) **Description**: Enter whatever you want to mark the alarm rule.

2. Select an object to be monitored and set alarm rule parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 8-1 Alarm rule parameters

Parameter	Description	Example Value
Resource Type	Type of the resource for which the alarm rule is configured. The resource type can only be **EIP and Bandwidth**.	Elastic IP and Bandwidth
Dimension	Metric dimension of the selected resource type. The dimension can only be **Bandwidth**.	Bandwidth
Monitoring Scope	Monitoring scope the alarm rule applies to. The only option is **Specific resources**. Select one or more objects and click » to synchronize them to the right pane.	Specific resources
Threshold Type	Type of the threshold. Only static thresholds are supported. A static threshold is a fixed threshold set in the alarm rule. If the metric reaches the configured threshold, an alarm is triggered.	Static
Method	The way that you set static thresholds. The only option is **Create manually**.	Create manually
Alarm Policy	Policy for triggering an alarm. Set the metric name, alarm policy, and alarm severity based on your requirements. The last part of the alarm policy indicates how often to trigger an alarm again when the alarm has been triggered but the monitored object is still abnormal. You can add a maximum of 20 alarm policies at a time.	Metric Name: Inbound Bandwidth Alarm Policy: If the raw value is greater than 210 Mbit/s for two consecutive periods, an alarm is generated every day. Alarm Severity: Major

3. Configure the alarm notification.

 Copyright © Huawei Technologies Co., Ltd.

Table 8-2 Alarm notification parameters

Parameter	Description	Example Value
Alarm Notification	Whether to notify users by sending emails or text messages.	Enable
Recipient	Alarms can be sent through notification groups.	Notification Group
Notification Group	Select the notification group that needs to receive alarm notifications. **Configure an alarm notification** if the notification group that you want to select does not exist.	-
Validity Period	IEC sends notifications only within the validity period specified in the alarm rule. If **Validity Period** is set to **08:00-20:00**, IEC sends notifications only within 08:00-20:00.	08:00-20:00
Trigger Condition	Condition for triggering the alarm notification. Select **Generated alarm** when an alarm is generated or **Cleared alarm** when an alarm is triggered, or both.	Generated alarm and Cleared alarm

4. Click **Create**.

   In the navigation pane on the left, choose **Alarm Management** > **Alarm History**. On the displayed page, view recent alarms.

----End

8.2 Managing Alarm Rules

Viewing Alarm Rule Information

In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**. On the displayed page, view alarm rule information.

 Copyright © Huawei Technologies Co., Ltd.

Table 8-3 Alarm rule information

Parameter	Description
Name/ID	• **Name**: Name of the alarm rule. The name was randomly generated by the system or set by you during alarm rule creation. You can click the name to go to its details page. • **ID**: Automatically generated by the system.
Resource Type	Type of the resource for which the alarm rule is configured. The resource type can only be **EIP and Bandwidth**.
Monitored Object	Name of the object monitored by the alarm rule.
Alarm Policy	Condition under which an alarm is generated for the resource.
Status	Status of an alarm rule. The status can be **Enabled** or **Disabled**. By default, an alarm rule that is just created is in the **Enabled** status.
Notification Group	Name of the notification group that receives alarm notifications.

Modifying an Alarm Rule

You can modify the name and description of an alarm rule as required, add a monitored object or remove a monitored object, and modify the alarm policy and alarm notification. Use either of the following two methods to modify an alarm rule:

- On the **Alarm Rules** page, locate the alarm rule and click **Modify** in the **Operation** column.
- Click the name of the alarm rule you want to modify. On the displayed page, click **Modify** in the upper right corner.

Enabling an Alarm Rule

- On the **Alarm Rules** page, locate the alarm rule and click **Enable** in the **Operation** column. In the displayed **Enable Alarm Rule** dialog box, click **Yes**.
- If you want to enable multiple alarm rules, select the alarm rules and click **Enable** in the upper left of the alarm rule list. In the displayed **Enable Alarm Rule** dialog box, click **Yes**.

Disabling an Alarm Rule

- On the **Alarm Rules** page, locate the alarm rule and click **Disable** in the **Operation** column. In the displayed **Disable Alarm Rule** dialog box, click **Yes**.
- If you want to disable multiple alarm rules, select the alarm rules and click **Disable** in the upper left of the alarm rule list. In the displayed **Disable Alarm Rule** dialog box, click **Yes**.

 Copyright © Huawei Technologies Co., Ltd.

Deleting an Alarm Rule

- On the **Alarm Rules** page, locate the alarm rule click **More** > **Delete** in the **Operation** column. In the displayed **Delete Alarm Rule** dialog box, click **Yes**.
- If you want to delete multiple alarm rules, select the alarm rules and click **Delete** in the upper left of the alarm rule list. In the displayed **Delete Alarm Rule** dialog box, click **Yes**.

8.3 Configuring an Alarm Notification

Scenarios

This section describes how to create notification groups and notification objects to notify specified users of alarms reported by the system so that they can handle faults in a timely manner.

Creating a Notification Group

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Alarm Management** > **Alarm Notifications**. On the displayed page, click **Notification Groups**.

Step 4 Click **Create Notification Group**.

Step 5 On the **Create Notification Group** page, set the parameters.

Table 8-4 Notification group parameters

Parameter	Description	Example Value
Group	Name of the notification group. The name can contain a maximum of 64 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.	group001

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Notification Objects	Notification objects contained in the notification group. A notification object can be added to multiple notification groups. Up to 10 notification objects can be added to a notification group at a time. If the notification object you want to select does not exist, choose **Alarm Notifications** > **Notification Objects** and **create a notification object**. IEC works with Simple Message Notification (SMN) to notify users of alarms. After the request for creating a notification group is submitted, a message will be sent to the endpoint set in each notification object to ask the users whether they would like to receive alarm notifications. A status will be displayed for each notification object on the notification group details page. A notification object can in one of the following three statuses: • **Confirmed**: The alarm notification request has been confirmed, and users will receive notifications through their endpoints when alarms are generated or cleared. • **Unconfirmed**: The alarm notification request has not been confirmed, and users will not receive notifications through their endpoints when alarms are generated or cleared. • **Canceled**: The alarm notification request has been confirmed but then canceled. If a notification object is in the **Unconfirmed** or **Canceled** status, you can click **Request Confirmation** in the **Operation** column to resend a message to the endpoint.	-

Step 6 Click **OK**.

----End

Creating a Notification Object

Step 1 Log in to the management console.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 In the navigation pane on the left, choose **Alarm Management** > **Alarm Notifications**. On the displayed page, click **Notification Objects**.

Step 4 Click **Create Notification Object**.

Step 5 On the **Create Notification Object** page, set the parameters.

- **Protocol**: Emails and SMS messages are supported.
- **Name**: Name of the notification object. The name can contain a maximum of 42 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
- **Endpoint**: A phone number or email address used to receive alarm notifications.

Step 6 Click **OK**.

----End

8.4 Managing Alarm Notifications

Viewing Notification Group Information

In the navigation pane on the left, choose **Alarm Management** > **Alarm Notifications**. On the displayed page, click **Notification Groups** and view the notification group information.

Table 8-5 Notification group information

Parameter	Description
Group/Topic Name	• **Group Name**: Name of the notification group, which was generated by system or set by you during notification group creation. Click the name to go to the details page to view more information or add or delete notification objects. • **Topic Name**: IEC works with SMN to provide subscription. A topic serves as a message sending channel, where publishers and subscribers can interact with each other. The topic name displayed here partially matches the subscription information received by the endpoint for easier alarm handling.
Notification Objects	Number of notification objects that were added to the notification group. Click **Add Notification Object** in the **Operation** column to add more notification objects to the notification group.
Created	Time when a notification group was created.
Last Modified	Last time when a notification group was modified.

 Copyright © Huawei Technologies Co., Ltd.

Modify a Notification Group

Locate the notification group you want to modify and click **Modify** in the **Operation** column.

Deleting a Notification Group

Locate the notification group you want to delete and click **Delete** in the **Operation** column.

Deleted notification groups cannot be recovered.

Viewing Notification Object Information

In the navigation pane on the left, choose **Alarm Management** > **Alarm Notifications**. On the displayed page, click **Notification Objects** and view the notification object information.

Table 8-6 Notification object information

Parameter	Description
Name	Name of the notification object, which was generated by system or set by you during notification object creation.
Protocol	Protocol used by the notification object. Emails and SMS messages are supported.
Endpoint	Phone number or email address to receive alarm notifications.
Notification Groups	Click **View Detail** to view all notification groups to which the notification object is added.

Deleting a Notification Object

Locate the notification object you want to delete and click **Delete** in the **Operation** column.

The notification object will be deleted from the notification group it belongs to and cannot be recovered.

8.5 Viewing the Alarm History

Scenarios

The alarm history displays the status changes of all alarm rules in the last 30 days and allows you to trace and view historical alarms.

Procedure

Step 1 Log in to the management console.

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.

The IEC **Overview** page is displayed.

Step 3 In the navigation pane on the left, choose **Alarm Management** > **Alarm History**. On the displayed page, check abnormal resources in the corresponding time period and handle the exceptions.

NOTE

- Typically, alarms are triggered based on calculation. Therefore, the alarm triggering time may be a few seconds later than the time the threshold was reached.
- If you have created or modified an alarm rule after obtaining the monitoring data and an alarm is triggered, the alarm triggering time is the time when you created or modified the alarm rule.

- On the **Alarm History** page, you can view the status changes of all alarm rules from the last 7 days. You can select a time range to search for the alarm history.
- You can also filter the alarms by resource ID or alarm rule name, and view alarms by status or severity.

  An alarm can be in any of the following statuses:

  - **Alarm**: The metric has triggered the alarm condition set in the alarm rule.
  - **Resolved**: The metric stops triggering the alarm condition set in the alarm rule.
  - **Insufficient data**: No monitoring data is reported for the metric set in the alarm rule for three consecutive hours. In special cases, if the monitoring data is reported at an interval longer than three hours and no monitoring data is reported for three consecutive periods, the alarm status also changes to **Insufficient data**.
  - **Invalid**: An alarm rule is modified or deleted.

Step 4 Locate the alarm you want to view and click **View Details** in the **Operation** column to view the detailed graph and alarm triggering information.

----End

 Copyright © Huawei Technologies Co., Ltd.

9 Quota Adjustment

What Are Quotas?

Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas limit the number or amount of resources available to users, for example, the maximum number of edge services and edge instances you can create.

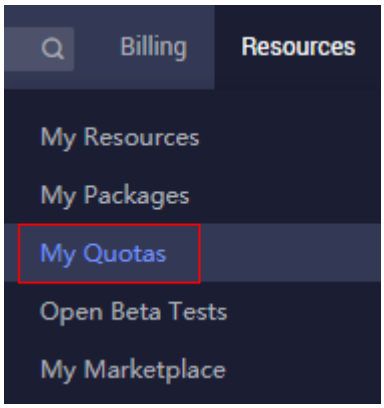
You can also increase the quota if the existing quota cannot meet your service requirements.

How Do I View My Quotas?

Step 1 Log in to the management console.

Step 2 In the upper right corner of the page, choose **Resources** > **My Quotas**.

The **Service Quota** page is displayed.



Step 3 View the used and total quota of each type of resources on the displayed page.

Step 4 If a quota cannot meet service requirements, apply for a higher quota.

----End

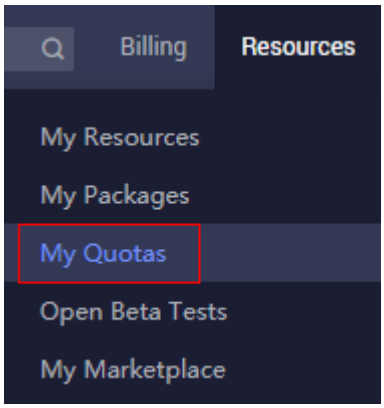
 Copyright © Huawei Technologies Co., Ltd.

How Do I Apply for a Higher Quota?

Step 1 Log in to the management console.

Step 2 In the upper right corner of the page, choose **Resources** > **My Quotas**.

The **Service Quota** page is displayed.



Step 3 Click **Increase Quota**.

Step 4 On the **Create Service Ticket** page, configure parameters as required.

Step 5 In the **Problem Description** area, enter the required quota and reason for the adjustment.

Step 6 After you configure all required parameters, select **I have read and agree to the Tenant Authorization Letter and Privacy Statement** and click **Submit**.

----End

 Copyright © Huawei Technologies Co., Ltd.

10 Common Operations

10.1 Deleting Files in the Network Rule Directory

Scenarios

To prevent NIC name drift on the edge instance you will create using a private image, you need to delete files in the network rule directory of the VM where the source edge instance is located during the private image creation.

Prerequisites

The xen-pv and virtio drivers have been installed on the edge instance.

Procedure

Step 1 View the files in the network rule directory.

ls -l /etc/udev/rules.d

Step 2 Delete the files with both **persistent** and **net** included in file names from the network rule directory.

Example:

rm /etc/udev/rules.d/*30-***net_persistent***-*names*.rules**

rm /etc/udev/rules.d/*70-***persistent-net.rules**

The italic content in the commands varies depending on your environment.

NOTE

For CentOS 6 images, to prevent NIC name drift, you need to create an empty rules configuration file.

Example:

touch /etc/udev/rules.d/*75-***persistent-net-generator.rules** //Replace *75* with the actual value in the environment.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 Delete network rules.

- If the OS uses the initrd system image, perform the following operations:
  a. Check whether the initrd image file whose name starts with **initrd** and ends with **default** contains the **persistent** and **net** network device rule files (replace the italic content in the following command with the actual OS version).

     lsinitrd /boot/initrd-*2.6.32.12-0.7*-default |grep persistent|grep net

     - If no, no further action is required.
     - If yes, go to **3.b**.

  b. Back up the initrd image files (replace the italic part in the following command with the actual OS version).

     cp /boot/initrd-*2.6.32.12-0.7*-default /boot/initrd-*2.6.32.12-0.7*-default_bak

  c. Generate the initrd file again.

     mkinitrd

- If the OS uses the initramfs system image (such as Ubuntu), perform the following operations:
  a. Check whether the initramfs image file whose name starts with **initrd** and ends with **generic** contains the **persistent** and **net** network device rule files.

     lsinitramfs /boot/initrd.img-3.19.0-25-generic|grep persistent|grep net

     - If no, no further action is required.
     - If yes, go to **3.b**.

  b. Back up the initrd image files.

     cp /boot/initrd.img-3.19.0-25-generic /boot/initrd.img-3.19.0-25-generic_bak

  c. Generate the initramfs image file again:

     update-initramfs -u

----End

10.2 Detaching Data Disks from an Edge Instance

Scenarios

If multiple data disks are attached to an edge instance used to create a private image, the edge instances created from the image may be unavailable. Therefore, you need to detach all data disks from the edge instance before you use it to create a private image.

This section describes how to detach all data disks from an edge instance.

Prerequisites

You have logged in to the edge instance used to create a Linux private image.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Check whether the edge instance has data disks.

Check the number of data disks attached to the edge instance.

fdisk -l

- If the number is greater than 1, the edge instance has data disks. Go to **2**.
- If the number is 1, no data disk is attached to the edge instance. Go to **3**.

Step 2 Check the data disks attached to the edge instance.

mount

- If the command output does not contain any data disk information, no data disks need to be detached.

```
/dev/vda1 on / type ext4 (rw,relatime,data=ordered)
```

- If information similar to the following is displayed, go to **3**.

```
/dev/vda1 on / type ext4 (rw,relatime,data=ordered)
/dev/vdb1 on /mnt/test type ext4 (rw,relatime,data=ordered)
```

Step 3 Delete the configuration information in the **fstab** file.

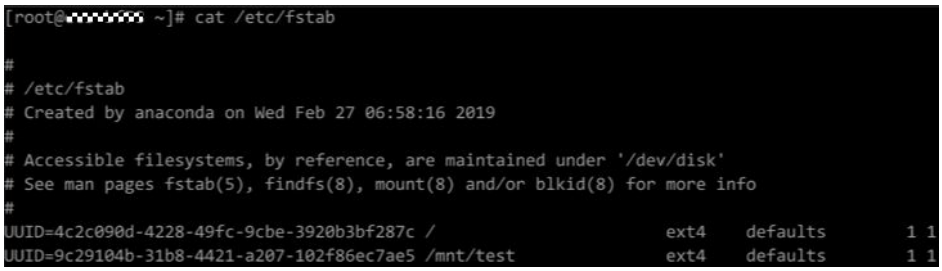
1. Edit the **fstab** file.

   vi /etc/fstab

2. Delete disk configuration from the **fstab** file.

   The **/etc/fstab** file contains information about the file systems and storage devices automatically attached to the edge instance when the edge instance starts. The configuration about data disks automatically attached to the edge instance needs to be deleted, for example, the last row shown in the following figure.

   Figure 10-1 Data disk configuration in the **fstab** file



Step 4 Detach data disks from the edge instance.

Ensure that no data read and write operations are being performed on the data disks that will be detached. Otherwise, the detaching operation will fail.

umount */dev/vdb1*

Step 5 Check the data disks attached to the edge instance.

mount

 Copyright © Huawei Technologies Co., Ltd.

If the command output contains no information about the data disks, they have been detached from the edge instance.

----End

10.3 Troubleshooting the Issue that a Key Pair Created Using puttygen.exe Cannot Be Imported to the Management Console

Symptom

When a key pair created using **puttygen.exe** was imported to the management console, the system displayed a message indicating that importing the public key failed.

Probable Causes

The format of the public key content does not meet system requirements.

Storing a public key by clicking **Save public key** of **puttygen.exe** will change the format of the public key content. Such a key cannot be imported to the management console.

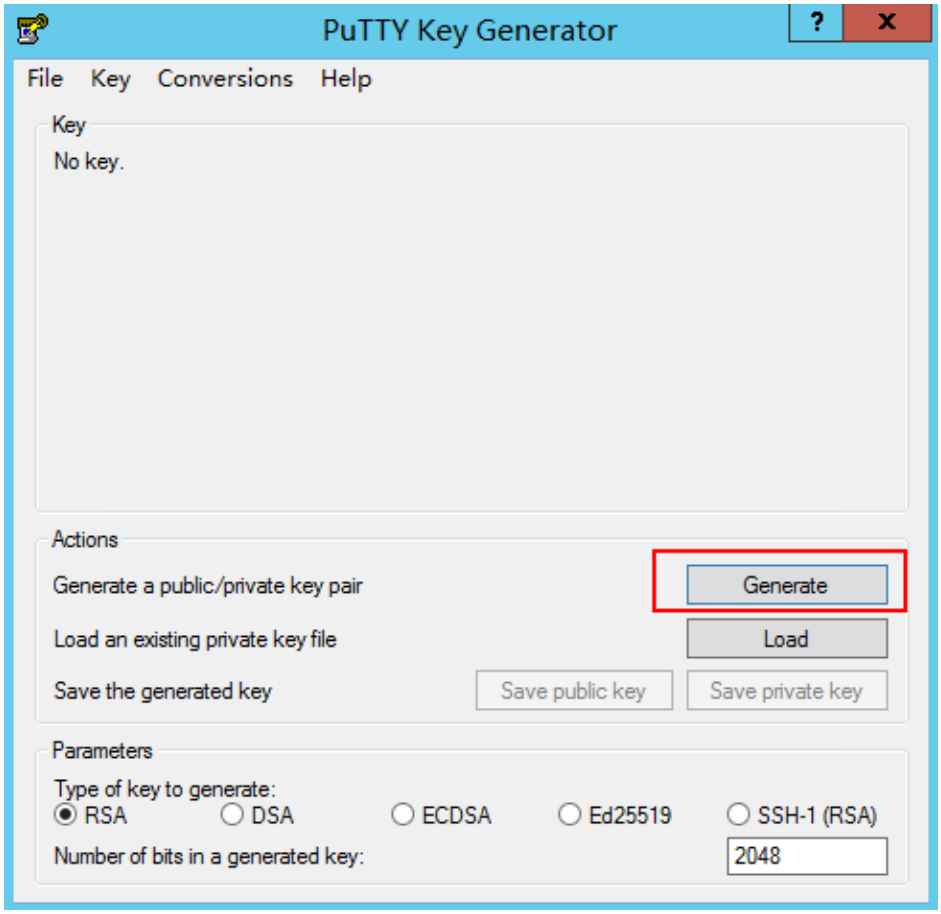
Solution

Use the locally stored private key and **PuTTY Key Generator** to restore the format of the public key content. Then, import the public key to the management console.

Step 1 Double-click **puttygen.exe** to switch to the **PuTTY Key Generator** page.

 Copyright © Huawei Technologies Co., Ltd.

Figure 10-2 PuTTY Key Generator

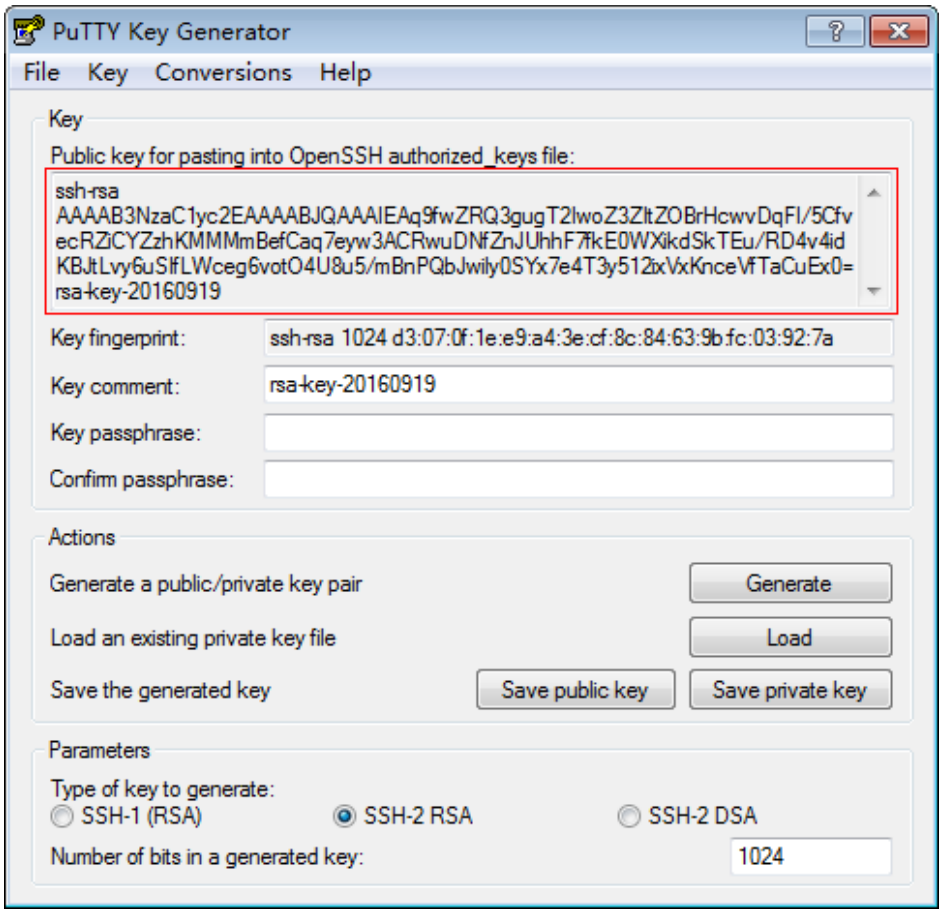


Step 2 Click **Load** and select the private key.

The system automatically loads the private key and restores the format of the public key content in **PuTTY Key Generator**. The content highlighted in red in **Figure 10-3** is the public key with the format meeting system requirements.

 Copyright © Huawei Technologies Co., Ltd.

Figure 10-3 Restoring the format of the public key content



Step 3 Copy the public key content and paste it to a .txt file and save the file in a local directory.

Step 4 Import the public key to the management console.

1. Log in to the management console.
2. Hover on the left menu to display **Service List**. Under **Content Delivery & Edge Computing**, select **Intelligent EdgeCloud**.
3. In the navigation pane on the left, choose **Key Pairs**.
4. On the right pane, click **Import Key Pair**.
5. Copy the public key content in the .txt file to **Public Key Content** and click **OK**.

----End

10.4 Configuring Policy-based Routing for an Edge Instance with Multiple NICs

Scenarios

If an edge instance has multiple NICs, you need to configure policy-based routing for the edge instance so that extension NICs are used for network communications.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

For a Linux edge instance:

Step 1 Add the priority value and name of the route table for each NIC to the **/etc/iproute2/rt_tables** file (a smaller value represents a higher priority. In this example, **250** and **net0** indicate the route table priority and the name of eth0, respectively. **251** and **net1** indicate the route table priority and the name of eth1, respectively. If there are multiple NICs, add the route table priority and the name of each NIC one by one).

vi /etc/iproute2/rt_tables

```
# added for dual net
250     net0
251     net1
```

Step 2 Add routing information of each NIC to the **rc.local** file.

vi /etc/rc.local

eth0 is used as an example here. If an IPv4 NIC is used, add the following information:

IPv4 address (192.168.0.129), subnet (192.168.0.0/24), gateway (192.168.0.1), and route table added in the preceding step (net0)

```
# wait for nics up
 sleep 5
 # Add v4 routes for eth0
 ip route flush table net0
 ip route add default via 192.168.0.1 dev eth0 table net0
 ip route add 192.168.0.0/24 dev eth0 table net0
 ip rule add from 192.168.0.129 table net0
 # Add v4 routes for eth1
 ip route flush table net1
 ip route add default via 192.168.1.1 dev eth1 table net1
 ip route add 192.168.1.0/24 dev eth1 table net1
 ip rule add from 192.168.1.138 table net1
```

Step 3 Add the execute permission to the **rc.local** file.

 # chmod +x /etc/rc.local

Step 4 Run **reboot** to restart the edge instance.

Step 5 After the restart, check whether the configured routes and route tables take effect.

For IPv4 NICs:

ip rule

ip route show table net0

ip route show table net1

 Copyright © Huawei Technologies Co., Ltd.

```
[root@ecs-3c3f ~]# ip rule
0:      from all lookup local
32764:  from 192.168.1.138 lookup net1
32765:  from 192.168.0.129 lookup net0
32766:  from all lookup main
32767:  from all lookup default
[root@ecs-3c3f ~]# ip route show table net0
default via 192.168.0.1 dev eth0
192.168.0.0/24 dev eth0 scope link
[root@ecs-3c3f ~]# ip route show table net1
default via 192.168.1.1 dev eth1
192.168.1.0/24 dev eth1 scope link
[root@ecs-3c3f ~]#
```

Step 6 Specify the source addresses for the test.

For IPv4 addresses:

ping -I 192.168.0.129 xxx

ping -I 192.168.1.138 xxx

----End

For a Windows edge instance:

Step 1 Choose **Control Panel** > **Network and Internet** > **Network Connections**. Right-click **Local Area Connection 2** and then click **Properties**.

NOTE

Right-click to add NICs based on the site requirements. If there are multiple NICs, there will be multiple local area connections. Configure them one by one.

Step 2 On the **Network** tab page, select **Internet Protocol Version 4 (TCP/IPv4)**.

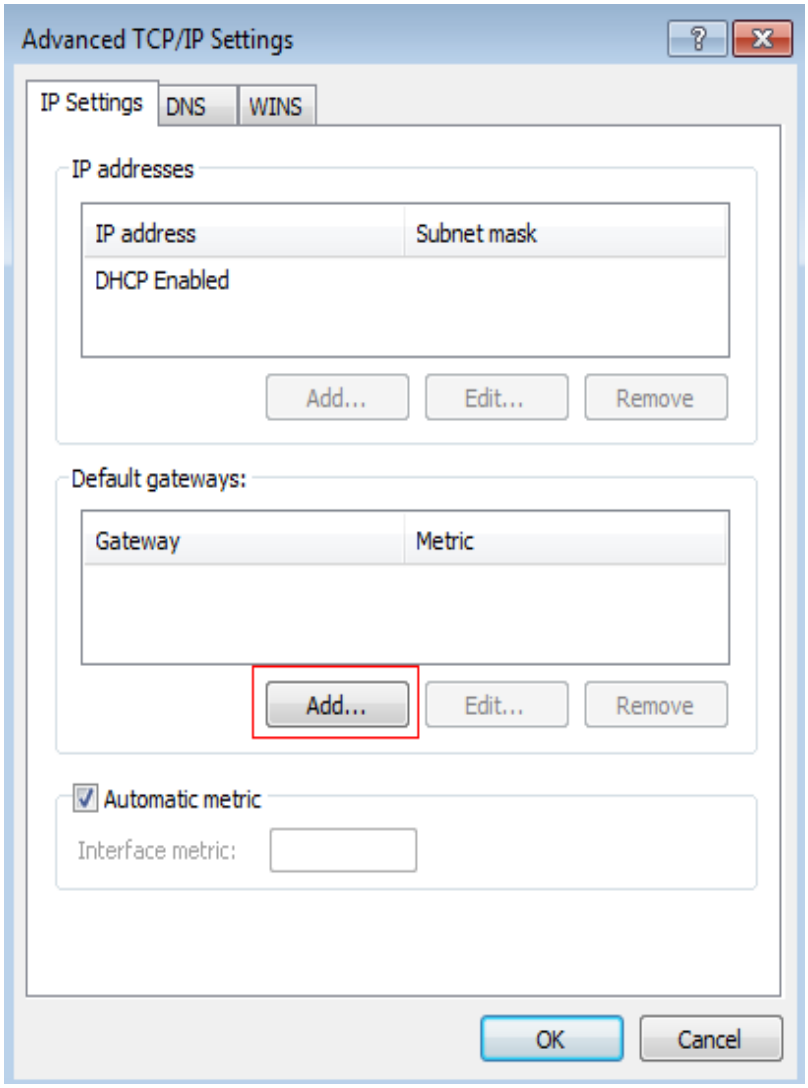
Step 3 Click **Properties**.

Step 4 On the **General** tab page, click **Advanced**.

Step 5 In the **IP Settings** tab, click **Add** in the **Default gateways** area.

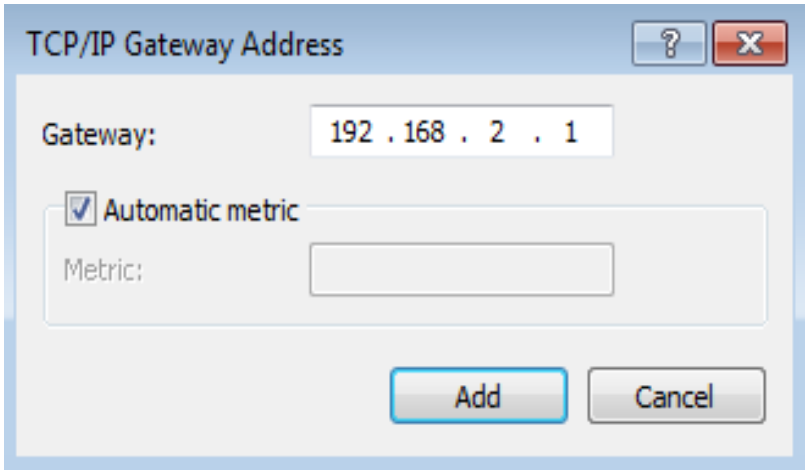
 Copyright © Huawei Technologies Co., Ltd.

Figure 10-4 Advanced TCP/IP settings



Step 6 Enter the gateway address of the extension NIC and click **Add**.

Figure 10-5 TCP/IP Gateway Address



 Copyright © Huawei Technologies Co., Ltd.

Step 7 Click **OK**.

Step 8 Open the command line interface (CLI) of the Windows OS and enter **route print** to view the policy-based routes.

```
C:\Users\Administrator>route print
===========================================================================
Interface List
  7...fa 16 3e 64 94 ae ......Red Hat VirtIO Ethernet Adapter
 29...fa 16 3e 00 42 c9 ......Red Hat VirtIO Ethernet Adapter #3
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.138    261
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.129      5
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  169.254.169.254  255.255.255.255    192.168.0.254    192.168.0.129      6
      192.168.0.0    255.255.255.0         On-link     192.168.0.129    261
    192.168.0.129  255.255.255.255         On-link     192.168.0.129    261
    192.168.0.255  255.255.255.255         On-link     192.168.0.129    261
      192.168.1.0    255.255.255.0         On-link     192.168.1.138    261
    192.168.1.138  255.255.255.255         On-link     192.168.1.138    261
    192.168.1.255  255.255.255.255         On-link     192.168.1.138    261
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link     192.168.0.129    261
        224.0.0.0        240.0.0.0         On-link     192.168.1.138    261
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
```

Step 9 Specify the source addresses for the test.

ping -S 192.168.0.129 xxx

ping -S 192.168.1.138 xxx

----End

Related Operations

Accessing the Internet using an EIP bound to an extension NIC

10.5 Accessing the Internet Using an EIP Bound to an Extension NIC

Step 1 After you bind an EIP to an extension NIC, access the edge instance and run **route** to query the routing information.

You can also run **route --help** to obtain the routing information.

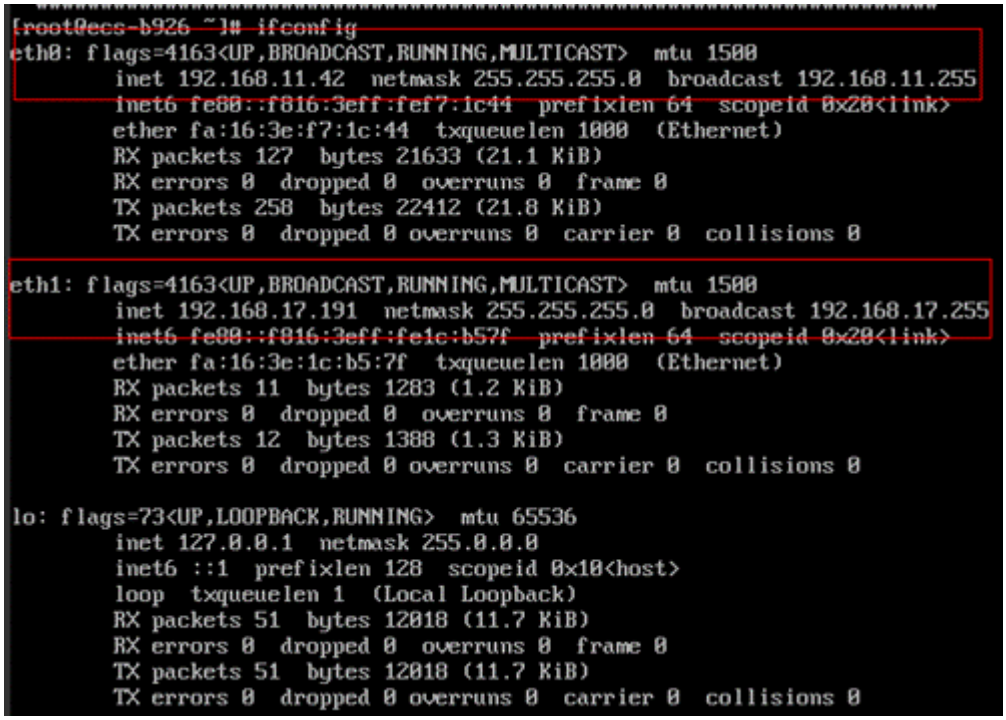
Figure 10-6 Viewing routing information

```
[root@ecs-b926 ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.11.1    0.0.0.0         UG    0      0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     1002   0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     1003   0        0 eth1
169.254.169.254 192.168.11.1    255.255.255.255 UGH   0      0        0 eth0
192.168.11.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.17.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
[root@ecs-b926 ~]#
```

Step 2 Run **ifconfig** to view NIC information.

 Copyright © Huawei Technologies Co., Ltd.

Figure 10-7 Obtaining the NIC information



Step 3 Configure Internet access from the extension NIC based on your destination address.

Configure access to a specified IP address range (for example, *xx.xx*.0.0/16) through the extension NIC.

route add -net xx.xx.0.0 netmask 255.255.0.0 gw 192.168.17.1

NOTE

If you want to use the extension NIC to access the Internet by default, run the following command:

This operation will interrupt network traffic. Exercise caution when performing this operation.

1. Delete the default route of the primary NIC.

   route del 0.0.0.0 192.168.11.1 dev eth0

2. Configure the default route for the extension NIC.

   route add default gw 192.168.17.1

----End

 Copyright © Huawei Technologies Co., Ltd.

A Change History

Released On	Description
2022-04-07	This issue is the twelfth official release, which incorporates the following changes: Added the function of batch deleting edge private images in "Deleting Edge Private Images." Changed the cloud database names in "Common Ports of Instances."
2021-12-07	This issue is the eleventh official release, which incorporates the following changes: Added parameters **Priority** and **Policy** to sections "Configuring Security Group Rules", "Managing Security Group Rules", and "Security Group Configuration Examples".
2021-10-13	This issue is the tenth official release, which incorporates the following changes: Added section "Auditing."
2021-09-13	This issue is the ninth official release, which incorporates the following changes: • Added the agency-related content in section "Creating an Edge Service". • Deleted parameter **Weekly Usage Peak** from section "Viewing Bandwidth Information". • Modified the method of viewing bandwidth monitoring data in section "Viewing Bandwidth and EIP Monitoring Data".
2021-08-17	This issue is the eighth official release, which incorporates the following changes: Added prerequisites in section "Deleting an Edge Service".

 Copyright © Huawei Technologies Co., Ltd.

Released On	Description
2021-08-06	This issue is the seventh official release, which incorporates the following changes: Added chapter "Alarms".
2021-07-31	This issue is the sixth official release, which incorporates the following changes: Optimized the description in section "Deleting a Bandwidth."
2021-07-01	This issue is the fifth official release, which incorporates the following changes: ● Added the descriptions and operations of changing a security group. ● Added a description that edge services can be batch deleted in section "Deleting an Edge Service". ● Added a description about the instance name prefix. ● Added two ECS types: general computing S6 and memory-optimized M6.
2021-06-08	This issue is the fourth official release, which incorporates the following changes: ● Optimized **Follow-up Operations** in section "Creating an Edge Service". ● Modified the descriptions of some parameters in section "Creating an Edge Service". ● Added sections "Viewing Edge Service Information", "Deleting an Edge Service", and "Managing VPCs".
2021-04-12	This issue is the third official release, which incorporates the following changes: ● Added section "Route Table". ● Added information that you can specify virtual IP addresses in section "Assigning a Virtual IP Address".
2021-01-30	This issue is the second official release, which incorporates the following changes: ● Added information about how to select a carrier line in section "Creating an Edge Service". ● Added the procedures of importing and exporting security group rules and network ACL rules.
2020-10-30	This issue is the first official release.

 Copyright © Huawei Technologies Co., Ltd.