VPC Endpoint

User Guide

Issue 01

Date 2025-01-14

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 VPC Endpoint Services

1.1 VPC Endpoint Service Overview

A VPC endpoint service is a cloud service or a private service that can be accessed through a VPC endpoint.

There are two types of VPC endpoint services: gateway and interface.

- Gateway VPC endpoint services are created only for cloud services.
- Interface VPC endpoint services can be created for both cloud services and your private services. Cloud services are configured as VPC endpoint services by the O&M personnel by default. However, you need to create VPC endpoint services for your private services.

NOTE

Supported cloud services vary in different regions. For details, see the services that can be configured on the management console.

You can configure OBS as a gateway VPC endpoint service on the VPC Endpoint console only in the LA-Mexico City1, LA-Sao Paulo1, and LA-Santiago regions.

To access OBS as gateway VPC endpoint services in other regions, you need to search for it by name. To obtain its name, you can **submit a service ticket** or contact the OBS O&M engineers.

This section describes how to configure a VPC endpoint service (interface type) from your private service and how to manage it.

Table 1-1 Management of VPC endpoint services

Operation	Description	Constraint
Creating a VPC Endpoint Service	Describes how to configure a private service as a VPC endpoint service.	● VPC endpoint services are region-level resources. Select a region and project when you create such a service. ● Each tenant can create a maximum of 20 VPC endpoint services. ● The following private services can be configured into VPC endpoint services: – **Elastic load balancer**: Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance. – **ECS**: Backend resources of this type serve as servers. – **BMS**: Backend resources of this type serve as servers. You can choose **BMS** when you choose **IPv4** for **Network Type**. ● One VPC endpoint service corresponds to only one backend resource.
Viewing a VPC Endpoint Service	Describes how to query details about a VPC endpoint service.	None
Deleting a VPC Endpoint Service	Describes how to delete a VPC endpoint service.	● Deleted VPC endpoint services cannot be recovered. Exercise caution when performing this operation. ● Only VPC endpoint services configured from users' private services can be deleted. ● VPC endpoint services in the **Accepted** or **Creating** state cannot be deleted.

Operation	Description	Constraint
Managing Connections of a VPC Endpoint Service	Describes how to set connection approval of a VPC endpoint service to determine whether to allow a VPC endpoint to connect to the VPC endpoint service.	You can specify whether to allow a VPC endpoint to connect to a VPC endpoint service only when connection approval is enabled during VPC endpoint service creation.
Managing Whitelist Records of a VPC Endpoint Service	Describes how to manage whitelist records of a VPC endpoint service to control across-account access between a VPC endpoint and a VPC endpoint service.	● The VPC endpoint and the VPC endpoint service must be deployed in the same region. ● Before you configure the whitelist for a VPC endpoint service, obtain the account ID of the associated VPC endpoint.
Managing Port Mappings of a VPC Endpoint Service	Describes how to view the port mapping between a VPC endpoint and a VPC endpoint service, including the supported protocol, service port, and terminal port.	● A port mapping needs to be configured when you create a VPC endpoint service. ● After a VPC endpoint service is created, you can view its port mappings but cannot modify them.
Managing Tags of a VPC Endpoint Service	Describes how to query, add, edit, and delete tags of a VPC endpoint service.	You can add up to 10 tags to each VPC endpoint service.

1.2 Creating a VPC Endpoint Service

Scenarios

There are two types of VPC endpoint services: gateway and interface.

- Gateway VPC endpoint services are created only for cloud services.
- Interface VPC endpoint services can be created for both cloud services and your private services. Cloud services are configured as VPC endpoint services by the O&M personnel by default. However, you need to create VPC endpoint services for your private services.

This section describes how to configure a private service into an interface VPC endpoint service.

Constraints

- VPC endpoint services are region-level resources. Select a region and project when you create such a service.

- Each tenant can create a maximum of 20 VPC endpoint services.
- The following private services can be configured into VPC endpoint services:
  - **Elastic load balancer**: Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance.
  - **ECS**: Backend resources of this type serve as servers.
  - **BMS**: Backend resources of this type serve as servers. You can choose **BMS** when you choose **IPv4** for **Network Type**.
- One VPC endpoint service corresponds to only one backend resource.

Prerequisites

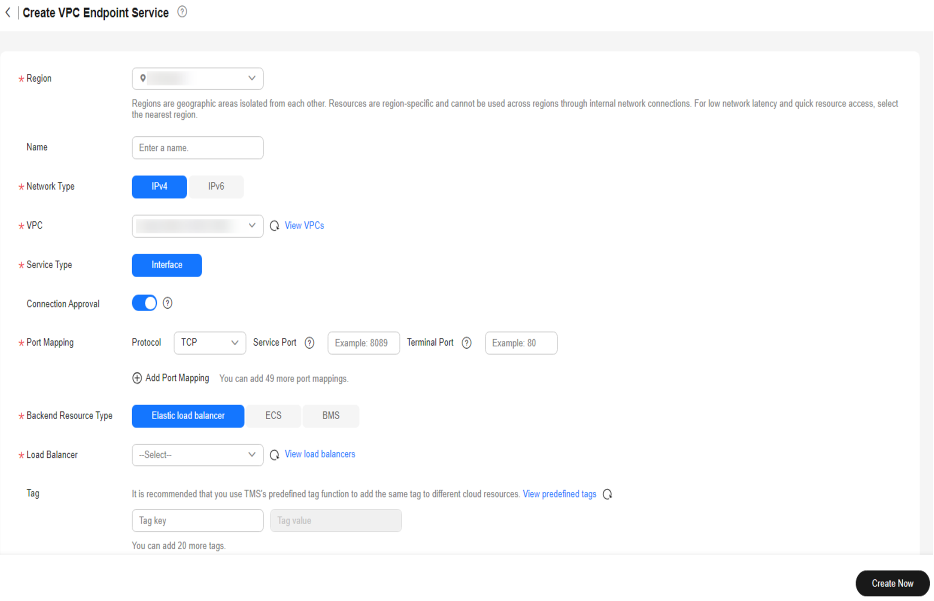
There is a load balancer in the VPC where you are going to create the VPC endpoint service.

Procedure

1. Go to the **VPC endpoint service list** page.
2. Click **Create VPC Endpoint Service**.

   The **Create VPC Endpoint Service** page is displayed.

   Figure 1-1 Create VPC Endpoint Service

   Create VPC Endpoint Service

   * Region
   Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

   Name: Enter a name.

   * Network Type: IPv4 | IPv6

   * VPC — View VPCs

   * Service Type: Interface

   Connection Approval

   * Port Mapping: Protocol TCP | Service Port Example: 8089 | Terminal Port Example: 80

   Add Port Mapping You can add 49 more port mappings.

   * Backend Resource Type: Elastic load balancer | ECS | BMS

   * Load Balancer: --Select-- — View load balancers

   Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags
   Tag key | Tag value
   You can add 20 more tags.

3. Configure parameters by referring to **Table 1-2**.

Table 1-2 Parameters for creating a VPC endpoint service

Parameter	Description
Region	Specifies the region where the VPC endpoint service is to be deployed. Resources in different regions cannot communicate with each other over an intranet. For lower latency and quicker access, select the nearest region.
Name	This parameter is optional. Specifies the name of the VPC endpoint service. The name can contain a maximum of 16 characters, including letters, digits, underscores (_), and hyphens (-). ● If you do not enter a name, the system generates a name in **{region}.{service_id}** format. ● If you enter a name, the system generates a name in **{region}.{Name}.{service_id}** format.
Network Type	Specifies the type of the VPC endpoint service. The value can be **IPv4** or **IPv6**. ● **IPv4**: Only IPv4 networks are supported. ● **IPv6**: Only IPv6 networks are supported.
VPC	Specifies the VPC where the VPC endpoint service is to be deployed.
Subnet	Specifies the subnet where the VPC endpoint service is to be deployed. This parameter is mandatory when you select **IPv6** for **Network Type**.
Service Type	Specifies the type of the VPC endpoint service. The type can only be **Interface**.
Connection Approval	Specifies whether the connection between a VPC endpoint and a VPC endpoint service requires approval from the owner of the VPC endpoint service. You can enable or disable **Connection Approval**. When **Connection Approval** is enabled, any VPC endpoint for connecting to the VPC endpoint service needs to be approved. For details, see **Managing Connections of a VPC Endpoint Service**.

Parameter	Description
Port Mapping	Specifies the protocol and ports used for communications between the VPC endpoint service and a VPC endpoint. The protocol is TCP or UDP. ● **Service Port**: provided by the backend resource bound to the VPC endpoint service. ● **Terminal Port**: provided by the VPC endpoint, allowing you to access the VPC endpoint service. The service and terminal port numbers range from **1** to **65535**. A maximum of 50 port mappings can be added at a time. NOTE Accessing a VPC endpoint service from a VPC endpoint is to access the service port from the associated terminal port.
Backend Resource Type	Specifies the backend resource that provides services to be accessed. The following backend resource types are supported: ● **Elastic load balancer**: Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance. ● **ECS**: Backend resources of this type serve as servers. ● **BMS**: Backend resources of this type serve as servers. You can choose **BMS** when you choose **IPv4** for **Network Type**. In this example, select **Elastic load balancer**. NOTE ● For the security group associated with the backend resource configured for the VPC endpoint service, add an inbound rule, with **Source** set to **198.19.128.0/17**. For details, see **Adding a Security Group Rule** in the *Virtual Private Cloud User Guide*. ● If you configure a load balancer as the backend resource for the VPC endpoint service, and enable access control for the listener associated with the load balancer, ensure to allow traffic from 198.19.128.0/17.
Load Balancer	When **Backend Resource Type** is set to **Elastic load balancer**, select the load balancer that provides services from the drop-down list. NOTE If an elastic load balancer is used as the backend resource, the source IP address received by the VPC endpoint service is not the real address of the client.
ECS List	This parameter is available when you select **ECS** for **Backend Resource Type**. Select an ECS from the ECS list.
BMS List	This parameter is available when you select **BMS** for **Backend Resource Type**. Select a BMS from the BMS list. NOTE The BMS type will be discarded. The ELB type is recommended.

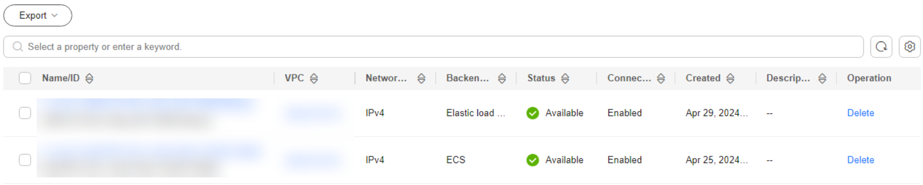
Parameter	Description
Tag	This parameter is optional. Specifies the VPC endpoint service tag, which consists of a key and a value. You can add up to 20 tags to each VPC endpoint service. Tag keys and values must meet requirements listed in **Table 1-3**. **NOTE** If a predefined tag has been created on TMS, you can directly select the corresponding tag key and value. For details about predefined tags, see **Predefined Tag Overview**. If you have configured tag policies for VPC Endpoint, add tags to VPC endpoint services based on the tag policies. If you add a tag that does not comply with the tag policies, VPC endpoint services may fail to be created. Contact your administrator to learn more about tag policies.
Description	Provides supplementary information about the VPC endpoint service.

Table 1-3 Tag requirements for VPC endpoint services

Parameter	Requirement
Tag key	● Cannot be left blank. ● Must be unique for each resource. ● Can contain a maximum of 36 characters. ● Can contain only letters, digits, hyphens (-), and underscores (_).
Tag value	● Cannot be left blank. ● Can contain a maximum of 43 characters. ● Can contain only letters, digits, hyphens (-), and underscores (_).

4. Click **Create Now**.
5. Click **Back to VPC Endpoint Service List** to view the newly-created VPC endpoint service.

Figure 1-2 VPC endpoint service list



Export

Select a property or enter a keyword.

□	Name/ID	VPC	Networ...	Backen...	Status	Connec...	Created	Descrip...	Operation
□	[redacted]	[redacted]	IPv4	Elastic load ...	✓ Available	Enabled	Apr 29, 2024...	--	Delete
□	[redacted]	[redacted]	IPv4	ECS	✓ Available	Enabled	Apr 25, 2024...	--	Delete

1.3 Viewing a VPC Endpoint Service

Scenarios

This section describes how to query details of a VPC endpoint service, including its name, ID, backend resource type, backend resource name, VPC, status, connection approval, service type, and creation time.

Procedure

1. Go to the **VPC endpoint service list** page.
2. Locate the VPC endpoint service by entering a filter in the search box in the upper right corner:
   - Search by name or ID.
     1. Select **Name** or **ID** in the filter box.
     2. Enter a keyword in the search box.
     3. Click 🔍 to start the search.

        VPC endpoint services containing the keyword are displayed.
   - Search by tag.
     1. Click ︾ to the right of **Search by Tag**.
     2. Enter a tag and a value.

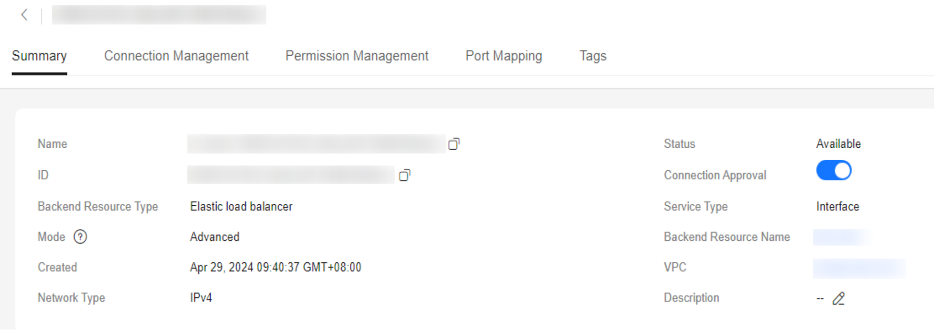
        You can also select a key or value from the drop-down list.

        You can use a maximum of 10 tags to search for a VPC endpoint service.
     3. Click **Search**.

        VPC endpoint services containing the specified tag are displayed.

        If you set multiple tags, VPC endpoint services containing all the specified tags will be displayed.
3. In the VPC endpoint service list, locate the VPC endpoint service and click its name to view its details.

Figure 1-3 Summary of the VPC endpoint service



Name [redacted]

ID [redacted]

Backend Resource Type Elastic load balancer

Mode Advanced

Created Apr 29, 2024 09:40:37 GMT+08:00

Network Type IPv4

Status Available

Connection Approval

Service Type Interface

Backend Resource Name [redacted]

VPC [redacted]

Description --

Table 1-4 describes the parameters displayed on the VPC endpoint service details page.

Table 1-4 Parameters contained in the details of a VPC endpoint service

Tab	Parameter	Description
Summary	Name	Specifies the name of the VPC endpoint service.
Summary	ID	Specifies the ID of the VPC endpoint service.
Summary	Backend Resource Type	Specifies the type of the backend resource that provides services.
Summary	Mode	Specifies the mode of the VPC endpoint service.
Summary	Network Type	Specifies the network type of the VPC endpoint service.
Summary	Backend Resource Name	Specifies the name of the backend resource that provides services to be accessed.
Summary	VPC	Specifies the VPC where the VPC endpoint service is to be deployed.
Summary	Status	Specifies the status of the VPC endpoint service.
Summary	Connection Approval	Specifies whether connection approval is required.
Summary	Service Type	Specifies the type of the VPC endpoint service.
Summary	Created	Specifies when the VPC endpoint service was created.
Connection Management	VPC Endpoint ID	Specifies the ID of the VPC endpoint.
Connection Management	Packet ID	Specifies the identifier of the VPC endpoint ID.
Connection Management	Status	Specifies the status of the VPC endpoint. For details about the statuses of a VPC endpoint, see **What Statuses Are Available for a VPC Endpoint Service and VPC Endpoint?**
Connection Management	Owner	Specifies the account ID of the VPC endpoint owner.

Tab	Parameter	Description
Connection Management	Created	Specifies the creation time of the VPC endpoint.
Connection Management	Operation	Specifies whether to allow a VPC endpoint to connect to a VPC endpoint service. The option can be **Accept** or **Reject**.
Permission Management	Authorized Account ID	Specifies the authorized account ID for connecting to the VPC endpoint. The ID can also be *. If you add an asterisk (*) to the whitelist, it means that all users can access the VPC endpoint service.
Permission Management	Operation	Specifies whether to delete an authorized account from the whitelist.
Port Mapping	Protocol	Specifies the protocol used for communications between the VPC endpoint service and a VPC endpoint.
Port Mapping	Service Port	Specifies the port provided by the backend service bound to the VPC endpoint service.
Port Mapping	Terminal Port	Specifies the port provided by the VPC endpoint, allowing you to access the VPC endpoint service.
Port Mapping	Operation	Specifies operations that will be performed on existing port mappings.
Tags	Key	Specifies the tag key of the VPC endpoint service.
Tags	Value	Specifies the tag value of the VPC endpoint service.
Tags	Operation	Specifies the operation to be performed on the VPC endpoint service tag. You can click **Edit** or **Delete**.

1.4 Deleting a VPC Endpoint Service

Scenarios

This section describes how you can delete a VPC endpoint service.

NOTE

Deleted VPC endpoint services cannot be recovered. Exercise caution when performing this operation.

Constraints

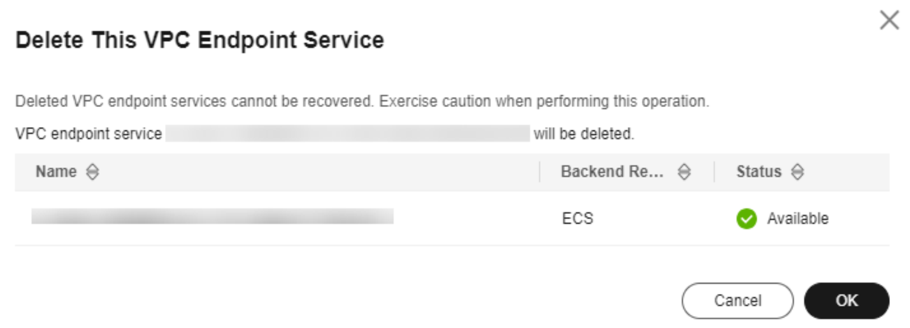
- The VPC endpoint services configured from your private services can be deleted, but those configured by the system cannot.
- Any VPC endpoint service that has VPC endpoints in **Accepted** or **Creating** state cannot be deleted.

  For statuses of a VPC endpoint, see **What Statuses Are Available for a VPC Endpoint Service and VPC Endpoint?**

Procedure

1. Go to the **VPC endpoint service list** page.
2. In the endpoint service list, locate the target endpoint service and click **Delete** in the **Operation** column.

   Figure 1-4 Deleting a VPC Endpoint Service

   Delete This VPC Endpoint Service

   Deleted VPC endpoint services cannot be recovered. Exercise caution when performing this operation.

   VPC endpoint service [redacted] will be deleted.

Name	Backend Re...	Status
[redacted]	ECS	Available

3. In the **Delete This VPC Endpoint Service** dialog box, click **OK**.

1.5 Managing Connections of a VPC Endpoint Service

Scenarios

To connect a VPC endpoint to a VPC endpoint service that has connection approval enabled, obtain the approval from the owner of the VPC endpoint service.

This section describes how to accept or reject a connection from a VPC endpoint.

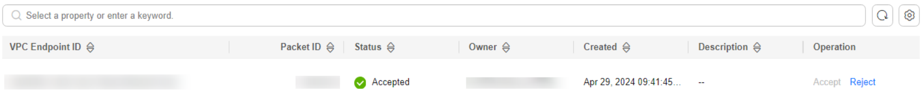
Prerequisites

- There is a VPC endpoint available for connecting to the target VPC endpoint service.
- **Connection Approval** of the VPC endpoint service is enabled.

Procedure

1. Go to the **VPC endpoint service list** page.
2. In the VPC endpoint service list, locate the VPC endpoint service and click its name.
3. Select the **Connection Management** tab.

Figure 1-5 Connection Management



VPC Endpoint ID	Packet ID	Status	Owner	Created	Description	Operation
[redacted]	[redacted]	Accepted	[redacted]	Apr 29, 2024 09:41:45...	--	Accept Reject

4. Accept or reject connection from a VPC endpoint in the list based on service requirements.
   - If you click **Accept**, the VPC endpoint can connect to the VPC endpoint service.
   - If you click **Reject**, the VPC endpoint cannot connect to the VPC endpoint service.

1.6 Managing Whitelist Records of a VPC Endpoint Service

Scenarios

Permission management controls the access of a VPC endpoint in one account to a VPC endpoint service in another.

After a VPC endpoint service is created, you can add or delete an authorized account ID to and from the whitelist of the VPC endpoint service.

- If the whitelist is empty, access from a VPC endpoint in another account is not allowed.
- If an authorized account ID is already in the whitelist, you can use this account to create a VPC endpoint for connecting to the VPC endpoint service.
- If an authorized account ID is not in the whitelist, you cannot use this account to create a VPC endpoint for connecting to the VPC endpoint service.

This section describes how to add or delete a whitelist record for a VPC endpoint service.

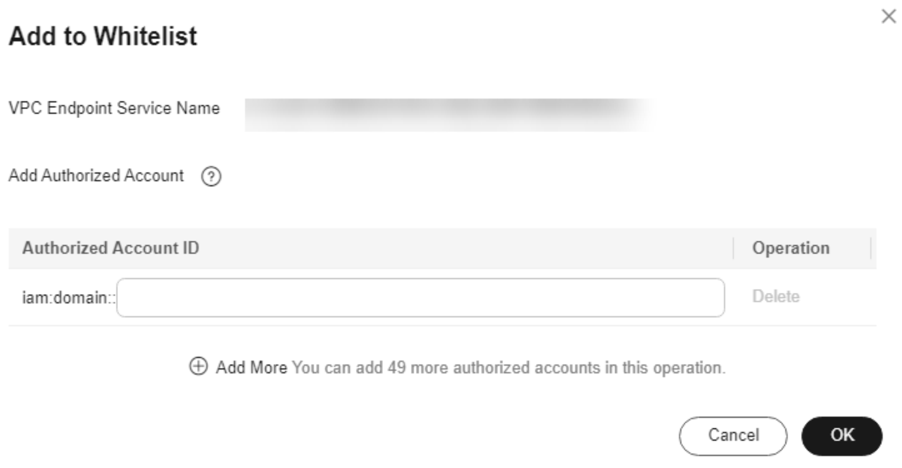
Constraints

- The VPC endpoint and the VPC endpoint service must be deployed in the same region.
- Before you configure the whitelist for a VPC endpoint service, obtain the account ID of the associated VPC endpoint.

Add a Whitelist Record

1. Go to the **VPC endpoint service list** page.
2. In the VPC endpoint service list, locate the VPC endpoint service and click its name.
3. On the displayed page, select the **Permission Management** tab and click **Add to Whitelist**.
4. Enter an authorized account ID in the required format and click **OK**.

Figure 1-6 Add to Whitelist



Add to Whitelist

VPC Endpoint Service Name

Add Authorized Account

Authorized Account ID	Operation
iam:domain::	Delete

⊕ Add More You can add 49 more authorized accounts in this operation.
Cancel
OK

NOTE

- Your account is in the whitelist of your VPC endpoint service by default.
- *domain_id* indicates the ID of the authorized account, for example, **1564ec50ef2a47c791ea5536353ed4b9**
- Adding ***** to the whitelist means that all users can access the VPC endpoint service.

Delete a Whitelist Record

1. In the VPC endpoint service list, locate the VPC endpoint service and click its name.
2. On the displayed page, click the **Permission Management** tab, locate the account ID, and click **Delete** in the **Operation** column.

   To delete multiple whitelist records, select all the target account IDs and click **Delete** in the upper left corner.
3. In the displayed **Delete from Whitelist** dialog box, click **OK**.

1.7 Managing Port Mappings of a VPC Endpoint Service

Scenarios

After a VPC endpoint service is created, you can add, modify, and view its port mappings.

You can view the protocol, service port, and terminal port.

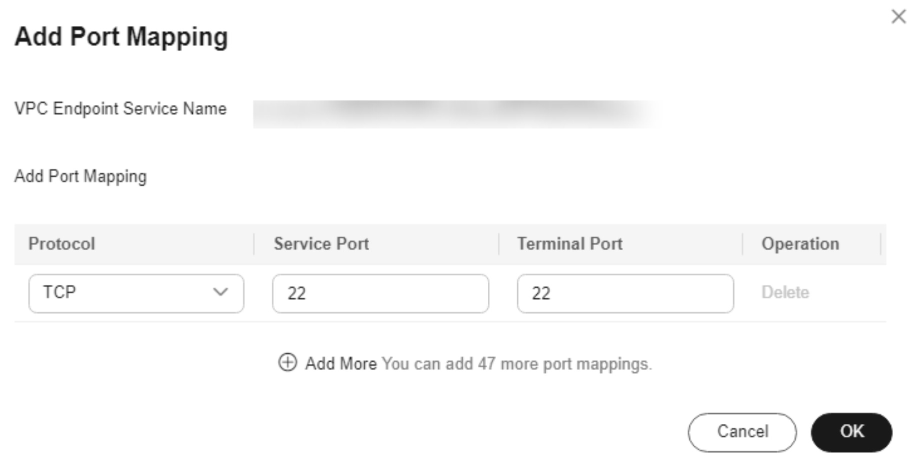
Adding a Port Mapping

1. Go to the **VPC endpoint service list** page.
2. In the VPC endpoint service list, locate the VPC endpoint service and click its name.

   The **Summary** tab of the VPC endpoint service is displayed.
3. Click the **Port Mapping** tab and click **Add Port Mapping**.

   Configure the parameters.

   Figure 1-7 Add Port Mapping



Add Port Mapping

VPC Endpoint Service Name [redacted]

Add Port Mapping

Protocol	Service Port	Terminal Port	Operation
TCP	22	22	Delete

⊕ Add More You can add 47 more port mappings.

4. Click **OK**.

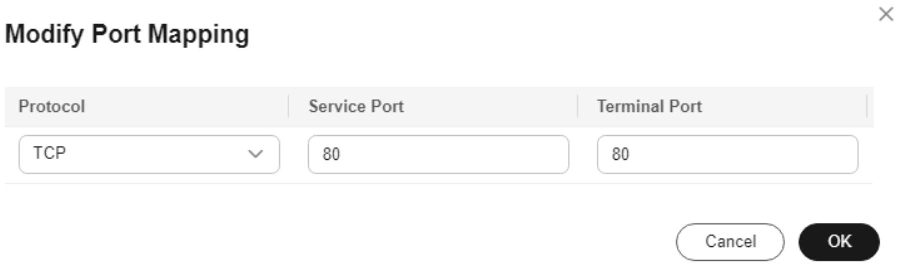
Modifying a Port Mapping

1. Go to the **VPC endpoint service list** page.
2. In the VPC endpoint service list, locate the VPC endpoint service and click its name.

   The **Summary** tab of the VPC endpoint service is displayed.
3. Click the **Port Mapping** tab, locate the port mapping, and click **Modify** in the **Operation** column.

   Configure the parameters.

Figure 1-8 Modify Port Mapping



Modify Port Mapping

Protocol	Service Port	Terminal Port
TCP	80	80

4. Click **OK**.

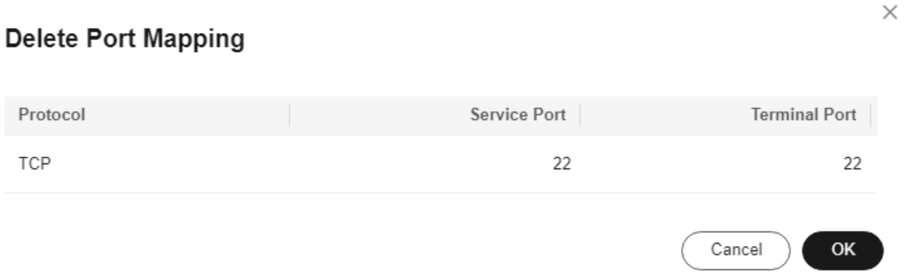
Deleting a Port Mapping

If a VPC endpoint service has only one port mapping, this port mapping cannot be deleted.

1. Go to the **VPC endpoint service list** page.
2. In the VPC endpoint service list, locate the VPC endpoint service and click its name.

   The **Summary** tab of the VPC endpoint service is displayed.
3. Click the **Port Mapping** tab, locate the port mapping, and click **Delete** in the **Operation** column.

Figure 1-9 Deleting a port mapping



Delete Port Mapping

Protocol	Service Port	Terminal Port
TCP	22	22

4. Confirm the information and click **OK**.

1.8 Managing Tags of a VPC Endpoint Service

Scenarios

After a VPC endpoint service is created, you can view its tags, or add, edit, or delete a tag.

Tags help identify VPC endpoint services. You can add up to 20 tags to each VPC endpoint service.

NOTE

If a predefined tag has been created on TMS, you can directly select the corresponding tag key and value.

For details about predefined tags, see **Predefined Tag Overview**.

If you have configured tag policies for VPC Endpoint, add tags to VPC endpoint services based on the tag policies. If you add a tag that does not comply with the tag policies, VPC endpoint services may fail to be created. Contact your administrator to learn more about tag policies.

Add a Tag

Perform the following operations to tag an existing VPC endpoint service:

1. Go to the **VPC endpoint service list** page.
2. In the VPC endpoint service list, locate the VPC endpoint service and click its name.
3. On the displayed page, select the **Tags** tab.
4. Click **Add Tag**.
5. In the displayed **Add Tag** dialog box, enter a key and a value.

   If you have configured tag policies for VPC Endpoint, add tags to VPC endpoint services based on the tag policies. If you add a tag that does not comply with the tag policies, VPC endpoint services may fail to be created. Contact your administrator to learn more about tag policies.

   Table 1-5 describes the tag requirements.

Table 1-5 Tag requirements for VPC endpoint services

Parameter	Requirement
Tag key	● Cannot be left blank. ● Must be unique for each resource. ● Can contain a maximum of 36 characters. ● Can contain only letters, digits, hyphens (-), and underscores (_).
Tag value	● Cannot be left blank. ● Can contain a maximum of 43 characters. ● Can contain only letters, digits, hyphens (-), and underscores (_).

6. Click **OK**.

Edit a Tag

Perform the following operations to edit a tag of a VPC endpoint service:

1. Go to the **VPC endpoint service list** page.
2. In the VPC endpoint service list, locate the VPC endpoint service and click its name.

3. On the displayed page, select the **Tags** tab.
4. In the tag list, locate the tag and click **Edit** in the **Operation** column.
5. Enter a new value.

   NOTE

   You can only edit tag values.
6. Click **OK**.

Delete a Tag

Perform the following operations to delete a tag of a VPC endpoint service:

CAUTION

Deleted tags cannot be recovered. Exercise caution when performing this operation.

1. Go to the **VPC endpoint service list** page.
2. In the VPC endpoint service list, locate the VPC endpoint service and click its name.
3. On the displayed page, select the **Tags** tab.
4. In the tag list, locate the tag and click **Delete** in the **Operation** column.
5. Click **OK**.

2 VPC Endpoints

2.1 VPC Endpoint Overview

VPC endpoints are secure and private channels for connecting VPCs to VPC endpoint services.

You can buy a VPC endpoint to connect a resource in your VPC to a VPC endpoint service in another VPC of the same region.

- VPC endpoints are classified into interface VPC endpoints and gateway VPC endpoints based on the types of VPC endpoint services they access.
  - **Interface VPC endpoints:** They access interface VPC endpoint services and are elastic network interfaces that have private IP addresses.
  - **Gateway VPC endpoints:** They access gateway VPC endpoint services and serve as gateways with routes configured to distribute traffic to the associated gateway VPC endpoint services.
- There are professional and basic VPC endpoints. Different editions have different features.
  - **Professional:** This newly released VPC endpoint type is available in the CN East2, ME-Riyadh, CN East-Qingdao, and AF-Cairo regions. A VPC endpoint supports up to 10 Gbit/s of bandwidth and IPv4 and IPv6 dual stack.
  - **Basic**: Basic VPC endpoints refer to previous VPC endpoints.

This section describes how to buy and manage a VPC endpoint.

Table 2-1 Management of VPC endpoints

Operation	Description	Constraint
Buying a VPC Endpoint	Describes how to buy a VPC endpoint.	- VPC endpoints are region-level resources. Select a region and project when you buy such a VPC endpoint. - Each tenant can buy a maximum of 50 VPC endpoints. - When you buy a VPC endpoint, ensure that the associated VPC endpoint service is deployed in the same region as the VPC endpoint. - Only one basic VPC endpoint can be created in a VPC subnet for accessing a VPC endpoint service. - When you create multiple VPC endpoints in a VPC to connect the same VPC endpoint service, you can enable **Create a Private Domain Name** for only one VPC endpoint. If you want to access multiple VPC endpoints using a private domain name, you need to modify the DNS record set. - VPC endpoints are billed based on the subscription duration.
Querying and Accessing a VPC Endpoint	Describes how to query the summary of a VPC endpoint.	The maximum number of concurrent connections supported by a VPC endpoint - Basic: 3,000 - Professional: 1,000,000
Deleting a VPC Endpoint	Describes how to delete a VPC endpoint.	Deleted VPC endpoints cannot be recovered. Exercise caution when performing this operation.

Operation	Description	Constraint
Configuring Access Control for an Interface VPC Endpoint	Describes how to enable access control for a VPC endpoint and configure a whitelist of IP addresses or CIDR blocks that are allowed to access the VPC endpoint.	● **Access Control** is only available for VPC endpoints for connecting to interface VPC endpoint services. ● If **Access Control** is disabled, any IP address can access the VPC endpoint. ● A maximum of 20 whitelist records can be added.
Managing Tags of a VPC Endpoint	Describes how to query, add, edit, and delete VPC endpoint tags.	You can add up to 10 tags to each VPC endpoint.

2.2 Buying a VPC Endpoint

Scenarios

VPC endpoints are secure and private channels for connecting VPCs to VPC endpoint services.

You can buy a VPC endpoint to connect a resource in your VPC to a VPC endpoint service in another VPC of the same region.

A VPC endpoint comes with a VPC endpoint service. VPC endpoints vary depending on the type of the VPC endpoint services that they can access.

- VPC endpoints for accessing interface VPC endpoint services are elastic network interfaces that have private IP addresses.
- VPC endpoints for accessing gateway VPC endpoint services are gateways, with routes configured to distribute traffic to the associated VPC endpoint services.

NOTE

VPC endpoints for accessing gateway VPC endpoint services can be purchased only in regions LA-Mexico City1, LA-Sao Paulo1, and LA-Santiago.

To access OBS as gateway VPC endpoint services in other regions, you need to search for it by name. To obtain its name, you can **submit a service ticket** or contact the OBS O&M engineers.

You can buy an interface or a gateway VPC endpoint based the type of the associated VPC endpoint service.

- **Buying a VPC Endpoint for Accessing Interface VPC Endpoint Services**
- **Buying a VPC Endpoint for Accessing Gateway VPC Endpoint Services**

Constraints

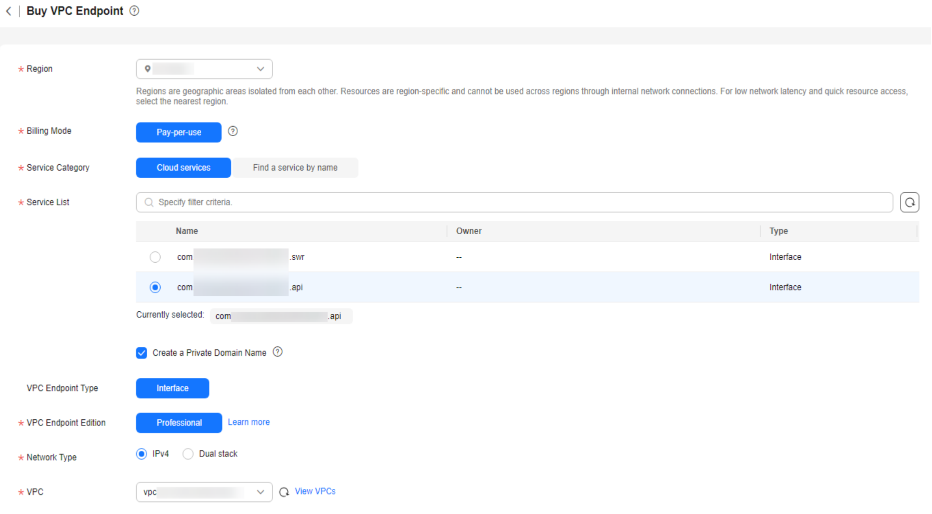
- VPC endpoints are region-level resources. Select a region and project when you buy such a VPC endpoint.

- Each tenant can buy a maximum of 50 VPC endpoints.
- When you buy a VPC endpoint, ensure that the associated VPC endpoint service is deployed in the same region as the VPC endpoint.
- Only one basic VPC endpoint can be created in a VPC subnet for accessing a VPC endpoint service.
- When you create multiple VPC endpoints in a VPC to connect the same VPC endpoint service, you can enable **Create a Private Domain Name** for only one VPC endpoint. If you want to access multiple VPC endpoints using a private domain name, you need to modify the DNS record set.
- VPC endpoints are billed based on the subscription duration.

Buying a VPC Endpoint for Accessing Interface VPC Endpoint Services

1. Go to the **VPC endpoint list** page.
2. On the **VPC Endpoints** page, click **Buy VPC Endpoint**.
3. On the **Buy VPC Endpoint** page, configure the parameters.

Figure 2-1 Buy VPC Endpoint (**Service Category** set to **Cloud services**)



< | Buy VPC Endpoint

* Region: [redacted]

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

* Billing Mode: Pay-per-use

* Service Category: Cloud services | Find a service by name

* Service List: Specify filter criteria.

	Name	Owner	Type
○	com[redacted].swr	--	Interface
●	com[redacted].api	--	Interface

Currently selected: com[redacted].api

☑ Create a Private Domain Name

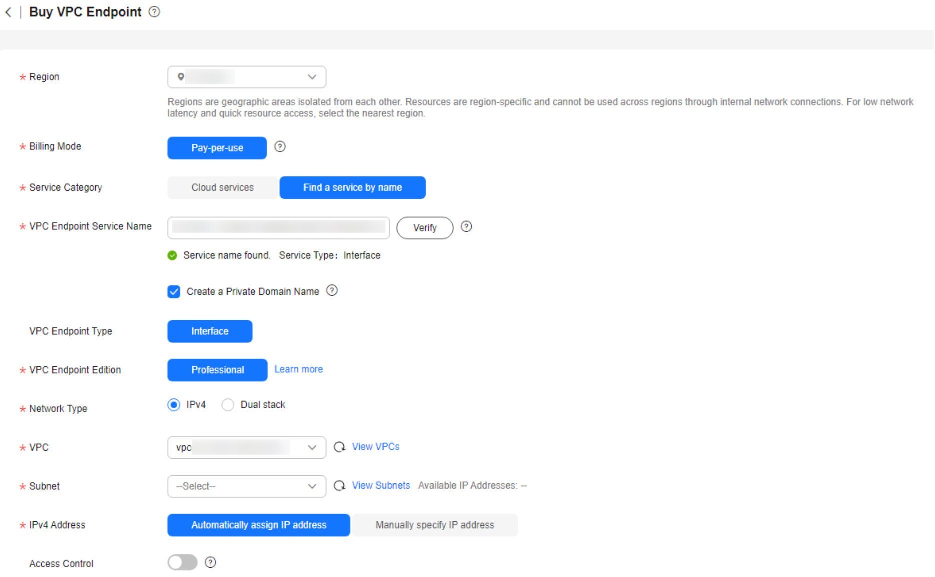
VPC Endpoint Type: Interface

* VPC Endpoint Edition: Professional Learn more

* Network Type: ● IPv4 ○ Dual stack

* VPC: vpc[redacted] View VPCs

Figure 2-2 Buy VPC Endpoint (**Service Category** set to **Find a service by name**)



Buy VPC Endpoint

* Region

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

* Billing Mode: Pay-per-use

* Service Category: Cloud services | Find a service by name

* VPC Endpoint Service Name: Verify

Service name found. Service Type：Interface

☑ Create a Private Domain Name

VPC Endpoint Type: Interface

* VPC Endpoint Edition: Professional Learn more

* Network Type: ● IPv4 ○ Dual stack

* VPC: vpc

* Subnet: --Select-- View Subnets Available IP Addresses: --

* IPv4 Address: Automatically assign IP address | Manually specify IP address

Access Control

Table 2-2 VPC endpoint parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint will be used to connect a VPC endpoint service. Resources in different regions cannot communicate with each other over an intranet. For lower latency and quicker access, select the region nearest to your on-premises data center.
Billing Mode	Specifies the billing mode of the VPC endpoint. VPC endpoints can be used or deleted at any time. VPC endpoints support only pay-per-use billing based on the usage duration.
Service Category	There are two options: ● **Cloud services**: Select this value if the target VPC endpoint service is a cloud service. ● **Find a service by name**: Select this value if the target VPC endpoint service is a private service of your own.
Service List	This parameter is available only when you select **Cloud services** for **Service Category**. The VPC endpoint service has been created by the O&M personnel and you can directly use it.

Parameter	Description
VPC Endpoint Service Name	This parameter is available only when you select **Find a service by name** for **Service Category**. In the VPC endpoint service list, locate the VPC endpoint service, copy its name in the **Name** column, paste it to the **VPC Endpoint Service Name** text box, and click **Verify**. ● If "Service name found." is displayed, proceed with subsequent operations. ● If "Service name not found." is displayed, check whether the region is the same as that of the VPC endpoint service or whether the name entered is correct.
Create a Private Domain Name	If you want to access a VPC endpoint using a domain name, select **Create a Private Domain Name**. This parameter is mandatory when the VPC endpoint will be used to access an interface VPC endpoint service.
VPC Endpoint Type	This parameter is displayed based on the type of the VPC endpoint service to be connected. ● If you are going to connect to an interface VPC endpoint service, **Interface** is displayed by default. ● If you are going to connect a gateway VPC endpoint service, **Gateway** is displayed by default.
VPC Endpoint Edition	This parameter is mandatory when you are going to connect to an interface VPC endpoint service. **Professional** is selected by default. **Professional** VPC endpoints are available in the CN East2, ME-Riyadh, CN East-Qingdao, and AF-Cairo regions. A VPC endpoint supports up to 10 Gbit/s of bandwidth and IPv4 and IPv6 dual stack.
Network Type	This parameter is mandatory when you are going to connecting to an interface VPC endpoint service whose **Mode** is **Advanced**. This parameter can be set to **IPv4** or **Dual stack**. ● **IPv4**: Only IPv4 networks are supported. ● **Dual stack**: Both IPv4 and IPv6 networks are supported.
VPC	Specifies the VPC where the VPC endpoint is to be deployed.
Subnet	This parameter is available when you want to access an interface VPC endpoint service. Specifies the subnet where the VPC endpoint is to be located.
IPv4 Address	IPv4 addresses can be automatically assigned or manually specified.

Parameter	Description
IPv6 Address	This parameter is mandatory when you select **Professional** for **VPC Endpoint Edition** and **Dual stack** for **Network Type**. IPv6 addresses can be automatically assigned or manually specified.
Access Control	This parameter is available when you want to access an interface VPC endpoint service. It controls IP addresses and CIDR blocks that are allowed to access the VPC endpoint. ● If **Access Control** is enabled, only IP addresses or CIDR blocks in the whitelist are allowed to access the VPC endpoint. ● If **Access Control** is disabled, any IP address or CIDR block can access the VPC endpoint.
Whitelist	This parameter is available when you want to access an interface endpoint service and **Access Control** is enabled. It lists the IP addresses or CIDR blocks that are allowed to access the VPC endpoint. You can add a maximum of 20 records. 0.0.0.0 and CIDR blocks in x.x.x.x/0 format are not supported.
Policy	Specifies the VPC endpoint policy. VPC endpoint policies are a type of resource-based policies. You can configure a policy to control which principals can use the VPC endpoint to access VPC endpoint services.
Tag	This parameter is optional. It specifies the VPC endpoint tag, which consists of a key and a value. You can add up to 20 tags to each VPC endpoint. Tag keys and values must meet requirements listed in **Table 2-3**. **NOTE** If a predefined tag has been created on TMS, you can directly select the corresponding tag key and value. For details about predefined tags, see **Predefined Tag Overview**. If you have configured tag policies for VPC Endpoint, add tags to this VPC endpoint based on the tag policies. If you add a tag that does not comply with the tag policies, VPC endpoints may fail to be created. Contact your administrator to learn more about tag policies.
Description	Provides supplementary information about the VPC endpoint service.

Table 2-3 Tag requirements for VPC endpoints

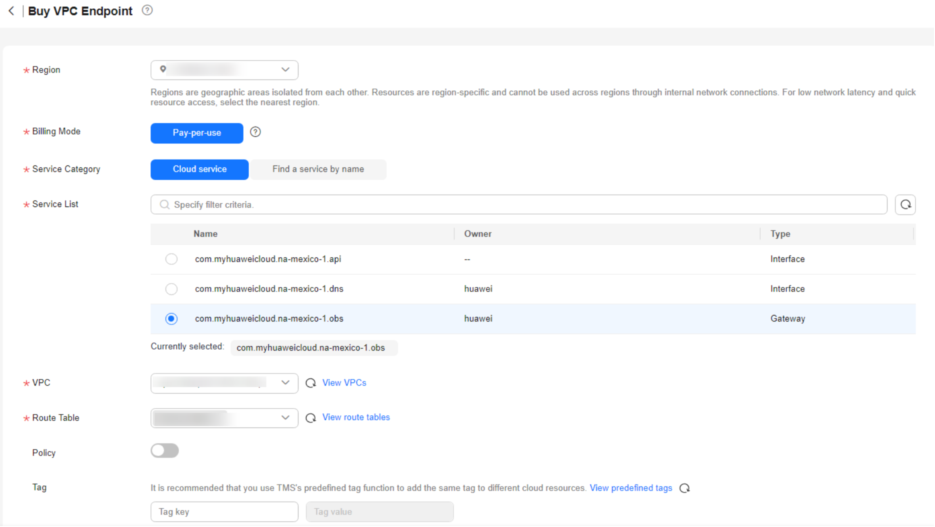
Parameter	Requirement
Tag key	● Cannot be left blank. ● Must be unique for each resource. ● Can contain a maximum of 36 characters. ● Can contain only letters, digits, hyphens (-), and underscores (_).
Tag value	● Cannot be left blank. ● Can contain a maximum of 43 characters. ● Can contain only letters, digits, hyphens (-), and underscores (_).

4. Confirm the settings and click **Next**.
   - If all of the settings are correct, click **Submit**.
   - If any of the settings are incorrect, click **Previous** to modify the parameter settings as needed, and click **Submit**.

Buying a VPC Endpoint for Accessing Gateway VPC Endpoint Services

1. Go to the **VPC endpoint list** page.
2. On the **VPC Endpoints** page, click **Buy VPC Endpoint**.
3. On the **Buy VPC Endpoint** page, configure the parameters.

Figure 2-3 Buy VPC Endpoint (**Service Category** set to **Cloud services**)



Buy VPC Endpoint

* Region

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

* Billing Mode: Pay-per-use

* Service Category: Cloud service | Find a service by name

* Service List: Specify filter criteria.

	Name	Owner	Type
○	com.myhuaweicloud.na-mexico-1.api	--	Interface
○	com.myhuaweicloud.na-mexico-1.dns	huawei	Interface
●	com.myhuaweicloud.na-mexico-1.obs	huawei	Gateway

Currently selected: com.myhuaweicloud.na-mexico-1.obs

* VPC: View VPCs

* Route Table: View route tables

Policy

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

Tag key | Tag value

Table 2-4 VPC endpoint parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint will be used to connect a VPC endpoint service. Resources in different regions cannot communicate with each other over an intranet. For lower latency and quicker access, select the region nearest to your on-premises data center.
Billing Mode	Specifies the billing mode of the VPC endpoint. VPC endpoints can be used or deleted at any time and support only pay-per-use billing based on the usage duration.
Service Category	There are two options: ● **Cloud services**: Select this value if the target VPC endpoint service is a cloud service. ● **Find a service by name**: Select this value if the target VPC endpoint service is a private service of your own.
Service List	This parameter is available only when you select **Cloud services** for **Service Category**. In the VPC endpoint service list, select the VPC endpoint service whose type is gateway. The VPC endpoint service has been created by the O&M personnel and you can directly use it. **NOTE** You can configure OBS as a gateway VPC endpoint service on the VPC Endpoint console only in the LA-Mexico City1, LA-Sao Paulo1, and LA-Santiago regions. Select the VPC endpoint service for OBS by region: ● LA-Mexico City1: com.myhuaweicloud.na-mexico-1.obs ● LA-Sao Paulo1: com.myhuaweicloud.sa-brazil-1.obs ● LA-Santiago: com.myhuaweicloud.la-south-2.obs To access OBS as gateway VPC endpoint services in other regions, you need to search for it by name. To obtain its name, you can **submit a service ticket** or contact the OBS O&M engineers.
VPC Endpoint Service Name	This parameter is available only when you select **Find a service by name** for **Service Category**. Enter the VPC endpoint service name recorded in **5** and click **Verify**. ● If "Service name found." is displayed, proceed with subsequent operations. ● If "Service name not found." is displayed, check whether the region is the same as that of the VPC endpoint service or whether the name entered is correct.
VPC	Specifies the VPC where the VPC endpoint is to be deployed.

Parameter	Description
Route Table	This parameter is available only when you create a VPC endpoint for connecting to a gateway VPC endpoint service. **NOTE** This parameter is available only in the regions where the route table function is enabled. Select all route tables. Or, the access to OBS may fail. Select a route table required for the VPC where the VPC endpoint is to be located. For details about how to add a route, see **Adding a Custom Route** in the *Virtual Private Cloud User Guide*.
Policy	Specifies the VPC endpoint policy. VPC endpoint policies are a type of resource-based policies. You can configure a policy to control which principals can use the VPC endpoint to access VPC endpoint services.
Tag	This parameter is optional. It specifies the VPC endpoint tag, which consists of a key and a value. You can add up to 20 tags to each VPC endpoint. Tag keys and values must meet requirements listed in **Table 2-5**. **NOTE** If a predefined tag has been created on TMS, you can directly select the corresponding tag key and value. For details about predefined tags, see **Predefined Tag Overview**. If you have configured tag policies for VPC Endpoint, add tags to this VPC endpoint based on the tag policies. If you add a tag that does not comply with the tag policies, VPC endpoints may fail to be created. Contact your administrator to learn more about tag policies.
Description	Provides supplementary information about the VPC endpoint service.

Table 2-5 Tag requirements for VPC endpoints

Parameter	Requirement
Tag key	● Cannot be left blank. ● Must be unique for each resource. ● Can contain a maximum of 36 characters. ● Can contain only letters, digits, hyphens (-), and underscores (_).

Parameter	Requirement
Tag value	● Cannot be left blank. ● Can contain a maximum of 43 characters. ● Can contain only letters, digits, hyphens (-), and underscores (_).

4. Confirm the settings and click **Next**.
   - If all of the settings are correct, click **Submit**.
   - If any of the settings are incorrect, click **Previous** to modify the parameter settings as needed, and click **Submit**.

2.3 Querying and Accessing a VPC Endpoint

Scenarios

After a VPC endpoint is bought, you can query its details and access it.

Constraints

The maximum number of concurrent connections supported by a VPC endpoint

- Basic: 3,000
- Professional: 1,000,000

Querying a VPC Endpoint

Perform the following operations to query details about a VPC endpoint, including its ID, associated VPC endpoint service name, VPC, and status.

1. Go to the **VPC endpoint list** page.
2. On the displayed page, locate the VPC endpoint by entering a keyword in the search box in the upper right corner:
   - Search by VPC endpoint service name or VPC endpoint ID.
     i. Select **ID** or **VPC Endpoint Service Name** in the filter box.
     ii. Enter a keyword in the search box.
     iii. Click 🔍 to start the search.
     VPC endpoints containing the keyword are displayed in the VPC endpoint list.
   - Search by tag.
     i. Click ︾ to the right of **Search by Tag**.
     ii. Enter a tag and a value.
     You can also select a key or value from the drop-down list.
     You can use a maximum of 10 tags to search for a VPC endpoint.

iii. Click **Search**.

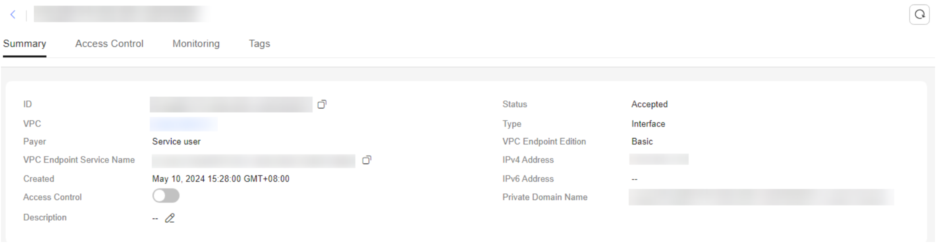
VPC endpoints containing the specified tag are displayed in the VPC endpoint list.

If you set multiple tags, VPC endpoints containing all the specified tags will be displayed.

3. In the VPC endpoint list, click the ID of the target VPC endpoint to view its details.

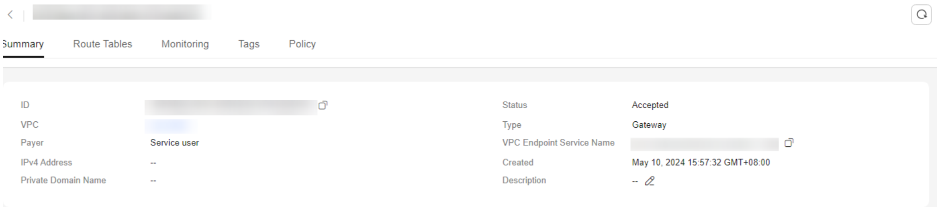
After an interface VPC endpoint is created, a private IP address is assigned together with a private domain name if you select **Create a Private Domain Name**.

Figure 2-4 Summary of the VPC endpoint (for accessing an interface VPC endpoint service)



ID [redacted]
VPC [redacted]
Payer Service user
VPC Endpoint Service Name [redacted]
Created May 10, 2024 15:28:00 GMT+08:00
Access Control
Description --
Status Accepted
Type Interface
VPC Endpoint Edition Basic
IPv4 Address [redacted]
IPv6 Address --
Private Domain Name [redacted]

Figure 2-5 Summary of the VPC endpoint (for accessing a gateway VPC endpoint service)



ID [redacted]
VPC [redacted]
Payer Service user
IPv4 Address --
Private Domain Name --
Status Accepted
Type Gateway
VPC Endpoint Service Name [redacted]
Created May 10, 2024 15:57:32 GMT+08:00
Description --

Table 2-6 Parameters contained in the details of a VPC endpoint

Tab	Parameter	Description
Summary	ID	Specifies the ID of the VPC endpoint.
Summary	VPC	Specifies the VPC where the VPC endpoint is deployed.
Summary	Payer	Specifies the payer of the VPC endpoint.
Summary	VPC Endpoint Service Name	Specifies the name of the VPC endpoint service that the VPC endpoint is used to access.
Summary	Private Domain Name	Specifies the private domain name for accessing the VPC endpoint.

Tab	Parameter	Description
Summary	Status	Specifies the status of the VPC endpoint.
Summary	Type	Specifies the type of the VPC endpoint service that the VPC endpoint is used to access.
Summary	VPC Endpoint Edition	Specifies the VPC endpoint edition.
Summary	IPv4 Address	Specifies the IPv4 address of the VPC endpoint.
Summary	IPv6 Address	Specifies the IPv6 address of the VPC endpoint.
Summary	Created	Specifies the creation time of the VPC endpoint.
Summary	Access Control	Specifies whether the whitelist is enabled for IP addresses to access this VPC endpoint. ● If **Access Control** is enabled, only IP addresses or CIDR blocks in the whitelist are allowed to access the VPC endpoint. ● If **Access Control** is disabled, any IP address or CIDR block can access the VPC endpoint. **NOTE** Access control can be enabled only for VPC endpoints for connecting to an interface VPC endpoint service.
Access Control	IP Address or CIDR Block	It controls IP addresses and CIDR blocks that are allowed to access the VPC endpoint. **NOTE** The **Access Control** tab is displayed only for VPC endpoints for connecting to interface VPC endpoint services.
Access Control	Operation	Specifies the operation to be performed on whitelist records of the VPC endpoint. Only deletion is supported.

Tab	Parameter	Description
Route Table	Name	Specifies the name of the route table. **NOTE** The **Route Tables** tab is displayed only for the VPC endpoint for connecting to a gateway VPC endpoint service in some specific regions.
Route Tables	VPC	Specifies the VPC that the route table belongs to.
Route Tables	Type	Specifies the type of the route table, which can be **Default** and **Custom**.
Route Tables	Associated Subnets	Specifies the number of subnets associated with the route table.
Route Tables	Operation	Specifies the operation to be performed on the route table. The operation can be **Disassociate** or **Associate**. **NOTE** If a VPC endpoint is associated with only one route table, disassociation is not supported.
Tags	Key	Specifies the tag key of the VPC endpoint.
Tags	Value	Specifies the tag value of the VPC endpoint.
Tags	Operation	Specifies the operation to be performed on the VPC endpoint tag. You can click **Edit** or **Delete**.

Accessing a VPC Endpoint via Its Private IP Address

Perform the following operations to access a VPC endpoint via its private IP address:

1. In the VPC where the VPC endpoint is deployed, log in to the backend resource, for example, an ECS.
2. Select a command based on the backend resource type and run the command to access the VPC endpoint. The command format is as follows:

   Command Private IP address:*Port number*

   The following is a command example:

   curl *Private IP address:Port number*

Accessing a VPC Endpoint via Its Private Domain Name

You can access a VPC endpoint via its private domain name if you select **Create a Private Domain Name** when buying the VPC endpoint.

The system automatically creates a private zone for the generated domain name and adds an A record set for the private zone to resolve the domain name into the private IP address of the VPC endpoint.

You can view the corresponding private zone and its resolution records on the DNS console.

Viewing the record set of the private domain name

1. Log in to the management console.
2. Hover the cursor over ≡ in the upper left corner. In the service list, choose **Networking** > **Domain Name Service**.

   The DNS console is displayed.
3. Go to the **VPC endpoint list** page.
4. In the private zone list, click the name of the target private zone.

   The **Record Sets** page is displayed.
5. In the record set list, locate the A record set and view its information.

   When **Status** changes to **Normal**, the resolution takes effect.

Accessing a VPC endpoint via its private domain name

1. In the VPC where the VPC endpoint is deployed, log in to the backend resource, for example, an ECS.
2. Select a command based on the backend resource type and run the command to access the VPC endpoint. The command format is as follows:

   Command Private domain name:*Port number*

   The following is a command example:

   curl *Private domain name:Port number*

2.4 Deleting a VPC Endpoint

Scenarios

This section describes how to delete a VPC endpoint.

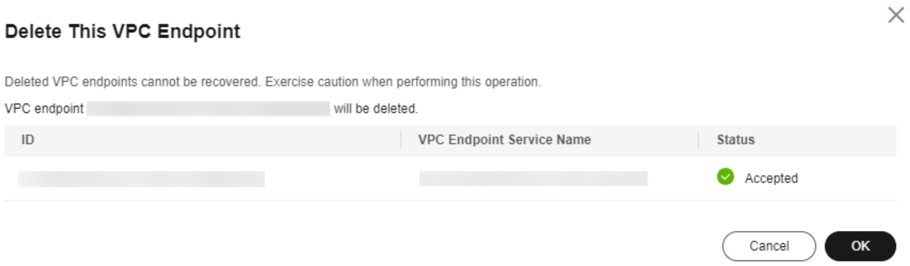
NOTE

Deleted VPC endpoints cannot be recovered. Exercise caution when performing this operation.

Procedure

1. Go to the **VPC endpoint list** page.
2. In the endpoint list, locate the target endpoint and click **Delete** in the **Operation** column.

Figure 2-6 Deleting a VPC endpoint



Delete This VPC Endpoint

Deleted VPC endpoints cannot be recovered. Exercise caution when performing this operation.

VPC endpoint [redacted] will be deleted.

ID	VPC Endpoint Service Name	Status
[redacted]	[redacted]	✓ Accepted

3. In the **Delete VPC Endpoint** dialog box, click **OK**.

2.5 Managing the Policy of a VPC Endpoint

VPC endpoint policies are a type of resource-based policies. You can configure a policy to control which principals can use the VPC endpoint to access Huawei Cloud services.

VPC endpoint policies do not override or replace the identity-based or resource-based policies in IAM. For example, if you have accessed OBS using a gateway VPC endpoint, you can still set OBS bucket policies to control access to an OBS bucket from a specific VPC endpoint or VPC.

There are two types of VPC endpoint policies:

- **Policies of gateway VPC endpoints**: policies that are configured to control which VPC endpoint can access gateway VPC endpoint services.
  - After this function is enabled, you can create custom policies. If you do not customize policies, the FullAccess policy is used by default.

    Default Policy:
    ```
    [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": [
                "*",
                "*/*"
            ]
        }
    ]
    ```
  - If this function is disabled, you cannot create custom policies.
- **Policies of interface VPC endpoints**: policies that are configured to control which VPC endpoint can access interface VPC endpoint services.
  - After this function is enabled, you can create custom policies. If you do not customize policies, the FullAccess policy is used by default.

    Default Policy:
    ```
    {
        "Version": "5.0",
        "Statement": [
            {
                "Effect": "Allow",
                "Principal": "*",
                "Action": [
                    "*"
    ```

```
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

- If this function is disabled, you cannot create custom policies.

Constraints

- A VPC endpoint policy is defined in the JSON document of IAM policies. VPC endpoint policies must comply with the grammar and structure of IAM permission policies.
- When creating an interface VPC endpoint for accessing a Huawei Cloud service, you can configure a policy for a single VPC endpoint and update the policy in real time. If you do not configure a VPC endpoint policy, full access is allowed for the VPC endpoint by default.
- Some Huawei Cloud services support VPC endpoint policies. For details, see the console. If a cloud service does not support VPC endpoint policies, the service can be accessed by any VPC endpoint.
- When you create a VPC endpoint for accessing a private service, full access is allowed for the VPC endpoint.

Configuring a Policy of a VPC Endpoint

You can enable **Policy** when buying a VPC endpoint. For details, see **Buying a VPC Endpoint**.

Viewing the Policy of a VPC Endpoint

1. Log in to the **VPC Endpoint console**.
2. Click 📍 in the upper left corner and select the desired region and project.
3. In the VPC endpoint list, click the VPC endpoint ID.
4. Click the **Policy** tab and view the VPC endpoint policy.

Modifying the Policy of a VPC Endpoint

1. Log in to the **VPC Endpoint console**.
2. Click 📍 in the upper left corner and select the desired region and project.
3. In the VPC endpoint list, click the VPC endpoint ID.
4. Go to the **Policy** tab, click **Edit** and modify the policy.
5. Click **Confirm**.

2.6 Configuring Access Control for an Interface VPC Endpoint

Scenarios

To control IP addresses and CIDR blocks that can access a VPC endpoint, configure a whitelist. You can add or delete a whitelist record, or disable access control if you no longer need it.

For details about how to configure access control and whitelist when you are buying a VPC endpoint, see **Buying a VPC Endpoint**.

This section describes how to enable and configure access control after a VPC endpoint is purchased.

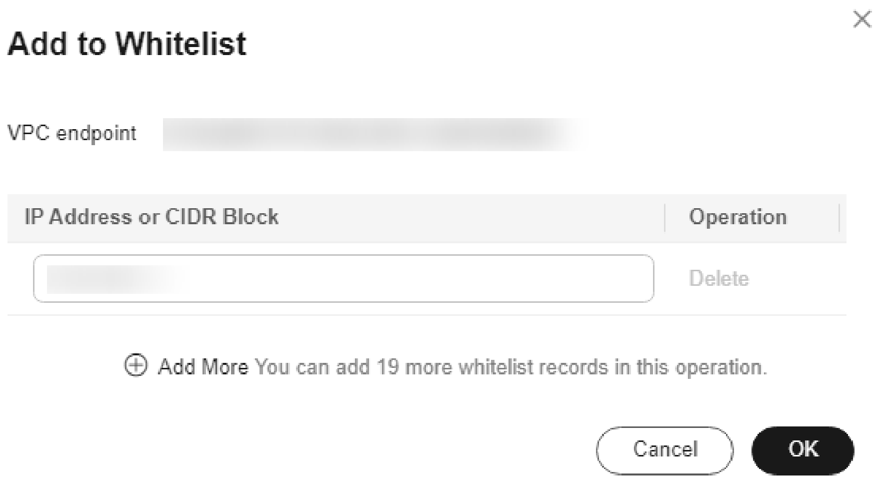
Constraints

- **Access Control** is only available for VPC endpoints for connecting to interface VPC endpoint services.
- If **Access Control** is disabled, any IP address can access the VPC endpoint.
- A maximum of 20 whitelist records can be added.

Enable Access Control and Add a Whitelist Record

1. Go to the **VPC endpoint list** page.
2. In the VPC endpoint list, locate the VPC endpoint and click its ID.
3. On the displayed page, click the **Access Control** tab.
4. On the **Access Control** tab, click **Add to Whitelist**.

Figure 2-7 Adding a whitelist record for the VPC endpoint



Add to Whitelist

VPC endpoint

IP Address or CIDR Block	Operation
	Delete

5. Enter the authorized IP addresses or CIDR blocks.

NOTE

A maximum of 20 whitelist records can be added for each VPC endpoint.

The asterisk (*) indicates all IP addresses or CIDR blocks can access the VPC endpoint. The current account is added to the whitelist by default.

6. Click **OK**.

Delete a Whitelist Record

1. Go to the **VPC endpoint list** page.
2. In the VPC endpoint list, locate the VPC endpoint and click its ID.
3. Select the **Access Control** tab.
4. In the whitelist, locate the IP address or CIDR block and click **Delete** in the **Operation** column.

   To delete whitelist records, select all the target IP addresses or CIDR blocks and click **Delete** in the upper left corner.
5. In the displayed **Delete from Whitelist** dialog box, click **OK**.

2.7 Configuring a Route Table for a Gateway VPC Endpoint

Scenarios

To establish secure and private channels for connecting a VPC to Huawei Cloud services, you can create a gateway VPC endpoint in this VPC, and associate a route table with the VPC endpoint. With a route table associated, the next hop of the cloud service is set to the gateway VPC endpoint so that the service can be accessed through the VPC endpoint.

This section describes how to associate or disassociate a route table with or from a VPC endpoint for connecting to a gateway VPC endpoint service.

⚠ CAUTION

- Disassociation cannot be done if a gateway VPC endpoint is associated with only one route table.
- Disassociating a route table from a VPC endpoint may hinder your services. Be careful with this operation.

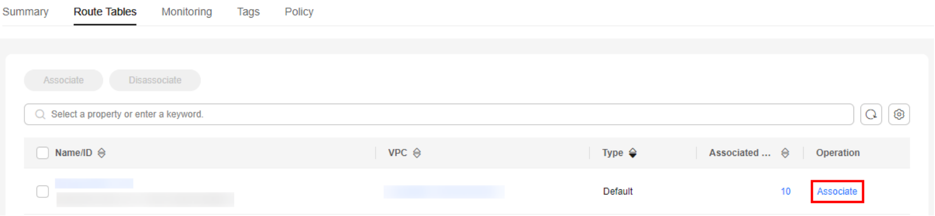
Constraints

Route tables can only be associated with VPC endpoints for connecting to gateway VPC endpoint services.

Associating a Route Table

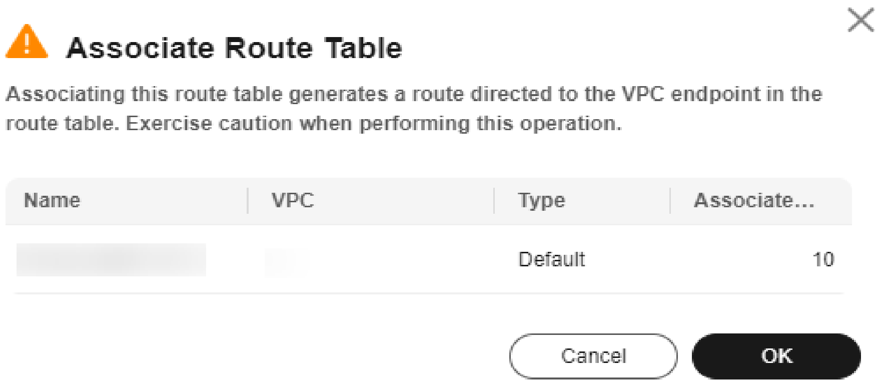
1. Go to the **VPC endpoint list** page.

2. In the VPC endpoint list, locate the VPC endpoint and click its ID.
3. On the **Route Tables** tab, click **Associate** in the **Operation** column of the target route table.



Name/ID	VPC	Type	Associated ...	Operation
[redacted]	[redacted]	Default	10	Associate

4. In the displayed dialog box, confirm the information and click **OK**.

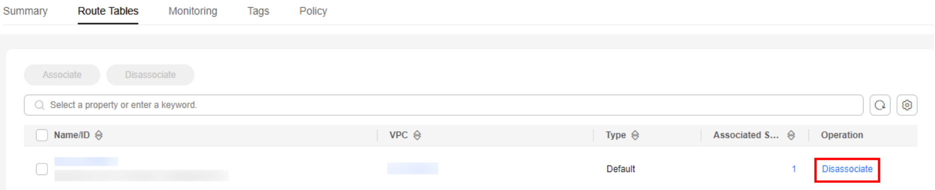

Associate Route Table

Associating this route table generates a route directed to the VPC endpoint in the route table. Exercise caution when performing this operation.

Name	VPC	Type	Associate...
[redacted]	[redacted]	Default	10

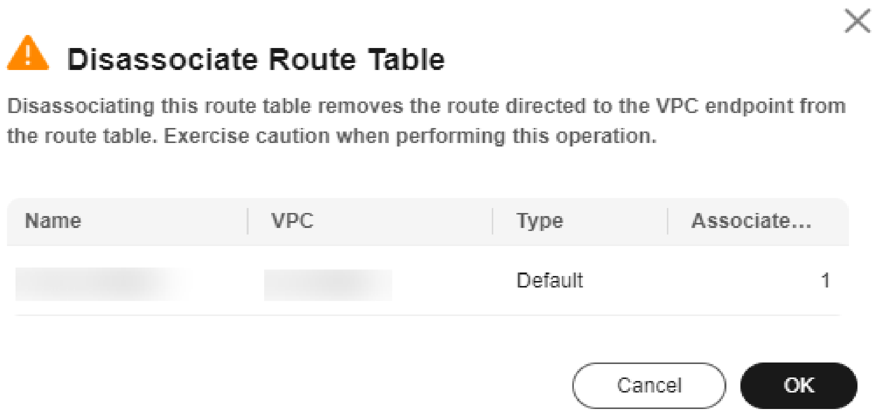
Disassociating a Route Table

1. Go to the **VPC endpoint list** page.
2. In the VPC endpoint list, locate the VPC endpoint and click its ID.
3. On the **Route Tables** tab, click **Disassociate** in the **Operation** column of the target route table.



Name/ID	VPC	Type	Associated S...	Operation
[redacted]	[redacted]	Default	1	Disassociate

4. In the displayed dialog box, confirm the information and click **OK**.



Disassociate Route Table

Disassociating this route table removes the route directed to the VPC endpoint from the route table. Exercise caution when performing this operation.

Name	VPC	Type	Associate...
[redacted]	[redacted]	Default	1

2.8 Managing Tags of a VPC Endpoint

Scenarios

After a VPC endpoint is created, you can view its tags, or add, edit, or delete a tag.

Tags help identify VPC endpoints. You can add up to 20 tags to each VPC endpoint.

NOTE

If a predefined tag has been created on TMS, you can directly select the corresponding tag key and value.

For details about predefined tags, see **Predefined Tag Overview**.

If you have configured tag policies for VPC Endpoint, add tags to this VPC endpoint based on the tag policies. If you add a tag that does not comply with the tag policies, VPC endpoints may fail to be created. Contact your administrator to learn more about tag policies.

Add a Tag

Perform the following operations to tag an existing VPC endpoint:

1. Go to the **VPC endpoint list** page.
2. In the VPC endpoint list, locate the VPC endpoint and click its ID.
3. On the displayed page, select the **Tags** tab.
4. Click **Add Tag**.
5. In the displayed **Add Tag** dialog box, enter a key and a value.

   If you have configured tag policies for VPC Endpoint, add tags to this VPC endpoint based on the tag policies. If you add a tag that does not comply with the tag policies, VPC endpoints may fail to be created. Contact your administrator to learn more about tag policies.

   Table 2-7 describes the tag requirements.

Table 2-7 Tag requirements for VPC endpoints

Parameter	Requirement
Tag key	● Cannot be left blank. ● Must be unique for each resource. ● Can contain a maximum of 36 characters. ● Can contain only letters, digits, hyphens (-), and underscores (_).
Tag value	● Cannot be left blank. ● Can contain a maximum of 43 characters. ● Can contain only letters, digits, hyphens (-), and underscores (_).

6. Click **OK**.

Edit a Tag

Perform the following operations to edit a tag of a VPC endpoint:

1. Go to the **VPC endpoint list** page.
2. In the VPC endpoint list, locate the VPC endpoint and click its ID.
3. On the displayed page, select the **Tags** tab.
4. In the tag list, locate the tag and click **Edit** in the **Operation** column.
5. Enter a new value.

   NOTE

   You can only edit tag values.
6. Click **OK**.

Delete a Tag

You can delete tags added to a VPC endpoint. Deleted tags cannot be restored. Exercise caution when performing this operation.

1. Go to the **VPC endpoint list** page.
2. In the VPC endpoint list, locate the VPC endpoint and click its ID.
3. On the displayed page, select the **Tags** tab.
4. In the tag list, locate the tag and click **Delete** in the **Operation** column.
5. Click **OK**.

3 Accessing OBS

Scenarios

This section describes how to access OBS using a VPN or Direct Connect connection.

NOTE

OBS can be configured as a gateway VPC endpoint service on the VPC Endpoint console only in the LA-Mexico City1, LA-Sao Paulo1, and LA-Santiago regions.

To access OBS as gateway VPC endpoint services in other regions, you need to search for it by name. To obtain its name, you can **submit a service ticket** or contact the OBS O&M engineers.

Prerequisites

Your on-premises data center has been connected to your VPC using a VPN or Direct Connect connection.

- The VPC subnet that needs to communicate with the VPN gateway must include the OBS CIDR block. For details about how to obtain the OBS CIDR block, **submit a service ticket** or contact the OBS customer manager.

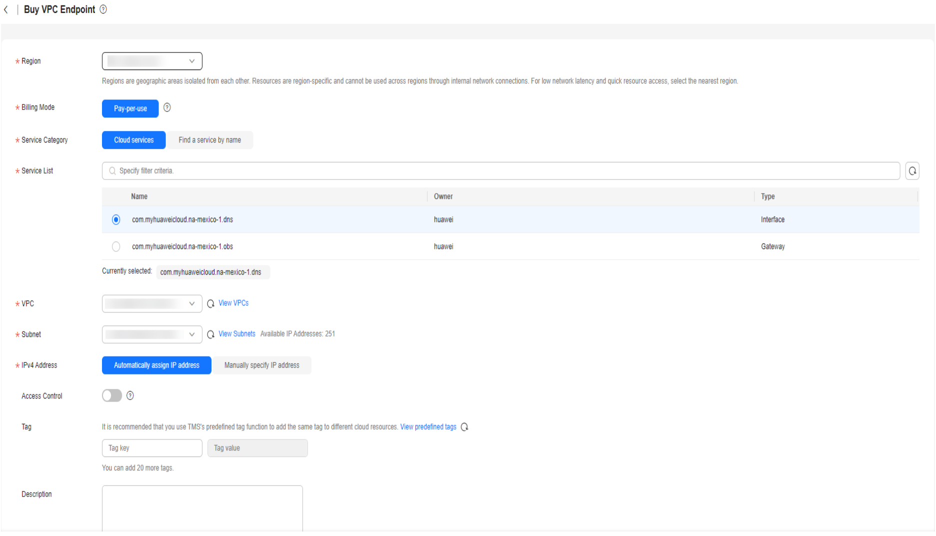
  For details about how to create a VPN connection, see **Creating a VPN Gateway**.

- The VPC subnet that needs to communicate with the Direct Connect virtual gateway must include the OBS CIDR block. For details about how to obtain the OBS CIDR block, **submit a service ticket** or contact the OBS customer manager.

  For details on how to enable Direct Connect, see **Enabling Direct Connect**.

Procedure

1. Go to the **VPC endpoint list** page.
2. On the displayed page, click **Buy VPC Endpoint**.
3. Set **Service Category** to **Cloud Services** and select **com.myhuaweicloud.na-mexico-1.dns**.
4. Configure required parameters.



Buy VPC Endpoint

* Region

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

* Billing Mode: Pay-per-use

* Service Category: Cloud services | Find a service by name

* Service List: Specify filter criteria.

	Name	Owner	Type
●	com.myhuaweicloud.na-mexico-1.dns	huawei	Interface
○	com.myhuaweicloud.na-mexico-1.obs	huawei	Gateway

Currently selected: com.myhuaweicloud.na-mexico-1.dns

* VPC: View VPCs

* Subnet: View Subnets Available IP Addresses: 251

* IPv4 Address: Automatically assign IP address | Manually specify IP address

Access Control

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

Tag key | Tag value

You can add 20 more tags.

Description

5. Click **Next** and **Submit**.
6. Check the private IP address returned after the VPC endpoint for connecting to DNS is created.
7. Add DNS records on the DNS server at your on-premises data center to forward requests for resolving OBS domain names to the VPC endpoint for accessing DNS.

   The methods of configuring DNS forwarding rules vary depending on OSs. For details, see the DNS software operation guides.

   This step uses Bind, a common DNS software, as an example to configure forwarding rules in the UNIX.

   Method 1: In file **/etc/named.conf**, add the DNS forwarder configuration and set **forwarders** to the private IP address of the VPC endpoint for accessing DNS.

```
options {
forward only;
forwarders{ xx.xx.xx.xx;};
};
```

   Method 2: In file **/etc/named.rfc1912.zones**, add the following content, and set **forwarders** to the private IP address of the VPC endpoint for accessing DNS.

   The following uses the OBS endpoint and cluster address of an OBS bucket in the LA-Mexico City1 region as an example:

```
zone "obs.na-mexico-1.myhuaweicloud.com" {
type forward;
forward only;
forwarders{ xx.xx.xx.xx;};
};
zone "obs.lz01.na-mexico-1.myhuaweicloud.com" {
type forward;
forward only;
forwarders{ xx.xx.xx.xx;};
};
```

NOTE

- If no DNS server is available at your on-premises data center, add the private IP address of the VPC endpoint in file **/etc/resolv.conf**.
- **obs.na-mexico-1.myhuaweicloud.com** indicates the OBS endpoint in the LA-Mexico City1 region.
- **obs.lz01.na-mexico-1.myhuaweicloud.com** indicates the address of the lz01 cluster where the OBS bucket is deployed.
- *xx.xx.xx.xx* indicates the IP address returned in step **9**.

8. Configure a DNS route from the on-premises node to the Direct Connect or VPN gateway.

   xx.xx.xx.xx indicates the private IP address of the VPC endpoint for accessing DNS. The traffic from the node to OBS needs to be directed to the Direct Connect or VPN gateway, and then to OBS through Direct Connect or VPN. Configure a permanent route at your on-premises data center and specify the IP address of the Direct Connect or VPN gateway as the next hop for accessing OBS.

   ```
   route -p add xx.xx.xx.xx mask 255.255.255.255 xxx.xxx.xxx.xxx
   ```

   NOTE

   - *xx.xx.xx.xx* indicates the IP address returned in step **9**.
   - *xxx.xxx.xxx.xxx* indicates the IP address of the Direct Connect or VPN gateway created at your on-premises data center.
   - The route command format varies depending on the OS. Use the route command format corresponding to the actual OS.

9. Repeat steps **5** to **9** to create a VPC endpoint for connecting to OBS.

   NOTE

   You can only access OBS using the OBS domain name in the region where the VPC endpoint is located.

10. Configure an OBS route from your on-premises data center to the Direct Connect or VPN gateway.

    The IP address of OBS belongs to 100.125.0.0/16. Traffic from the data center to OBS needs to be directed to the Direct Connect or VPN gateway, and then to OBS through Direct Connect or VPN.

    Configure a permanent route at your on-premises data center and specify the IP address of the Direct Connect or VPN gateway as the next hop for accessing OBS.

    ```
    route -p add 100.125.0.0 mask 255.255.0.0 xxx.xxx.xxx.xxx
    ```

    NOTE

    - If your on-premises data center is disconnected from the Direct Connect gateway or a VPN gateway, a connection between the on-premises node and the gateway must be established first.
    - The route command format varies depending on the OS. Use the route command format corresponding to the actual OS.

4 Using Cloud Eye to Monitor VPC Endpoints

4.1 Monitoring VPC Endpoints

Monitoring is key to ensuring performance, reliability, and availability of VPC endpoints. Cloud Eye helps you track statuses and performance of your VPC endpoints in real time.

NOTE

VPC Endpoint supports Cloud Eye in the CN East2, AF-Cairo, and CN Southwest-Guiyang1 (only some VPC endpoint metrics) regions. Check supported metrics on the management console.

This section covers the following content:

- **Supported Metrics**
- **Setting an Alarm Rule**
- **Viewing Metrics**

4.2 Supported Metrics

Description

This topic describes VPC Endpoint namespaces, the metrics that can be monitored by Cloud Eye, and dimensions of these metrics. You can log in to the Cloud Eye console or call Cloud Eye APIs to query the VPC endpoint metrics and alarms.

Namespace

SYS.VPCEP

Metrics

Table 4-1 VPC Endpoint metrics

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period
vpcep_rx_bps	Inbound Bandwidth	Inbound bandwidth of the VPC endpoint Unit: bit/s	≥ 0	VPC endpoint	60s
vpcep_tx_bps	Outbound Bandwidth	Outbound bandwidth of the VPC endpoint Unit: bit/s	≥ 0		60s
vpcep_bps	Inbound and Outbound Bandwidth	Inbound and outbound bandwidth of the VPC endpoint Unit: bit/s	≥ 0		60s
vpcep_rx_pps	Inbound PPS	Inbound PPS of the VPC endpoint Unit: Packets/s	≥ 0		60s
vpcep_tx_pps	Outbound PPS	Outbound PPS of the VPC endpoint Unit: Packets/s	≥ 0		60s
vpcep_pps	Inbound and Outbound PPS	Inbound and outbound PPS of the VPC endpoint Unit: Packets/s	≥ 0		60s
vpcep_rx_byte	Inbound Traffic	Inbound traffic of the VPC endpoint Unit: bytes	≥ 0		60s
vpcep_tx_byte	Outbound Traffic	Outbound traffic of the VPC endpoint Unit: bytes	≥ 0		60s

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period
vpcep_drop_num	Packets Dropped	Number of packets dropped by the VPC endpoint Unit: Packets	≥ 0		60s
vpcep_connections	Connections	Number of current connections established between the VPC endpoint and the VPC endpoint service it connects to Unit: Count	≥ 0		60s
vpcep_act_connections	Active Connections	Number of active connections established between the VPC endpoint and the VPC endpoint service it connects to Unit: Count	≥ 0		60s
vpcep_eps_rx_bps	Inbound Bandwidth	Inbound bandwidth of the VPC endpoint service Unit: bit/s	≥ 0	VPC endpoint service	60s
vpcep_eps_tx_bps	Outbound Bandwidth	Outbound bandwidth of the VPC endpoint service Unit: bit/s	≥ 0		60s

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period
vpcep_eps_bps	Inbound and Outbound Bandwidth	Inbound and outbound bandwidth of the VPC endpoint service Unit: bit/s	≥ 0		60s
vpcep_eps_rx_pps	Inbound PPS	Inbound PPS of the VPC endpoint service Unit: Packets/s	≥ 0		60s
vpcep_eps_tx_pps	Outbound PPS	Outbound PPS of the VPC endpoint service Unit: Packets/s	≥ 0		60s
vpcep_eps_pps	Inbound and Outbound PPS	Inbound and outbound PPS of the VPC endpoint service Unit: Packets/s	≥ 0		60s
vpcep_eps_rx_byte	Inbound Traffic	Inbound traffic of the VPC endpoint service Unit: bytes	≥ 0		60s
vpcep_eps_tx_byte	Outbound Traffic	Outbound traffic of the VPC endpoint service Unit: bytes	≥ 0		60s
vpcep_eps_drop_num	Packets Dropped	Number of packets dropped by the VPC endpoint service Unit: Packets	≥ 0		60s

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period
vpcep_eps_connections	Connections	Number of current connections established between the VPC endpoint service and all VPC endpoints connect to it Unit: Count	≥ 0		60s
vpcep_eps_act_connections	Active Connections	Number of active connections established between the VPC endpoint service and all VPC endpoints connect to it Unit: Count	≥ 0		60s

Dimension

Key	Value
ep_instance_id	VPC endpoint
eps_id	VPC endpoint service

4.3 Setting an Alarm Rule

Scenarios

You can configure alarm rules to customize monitored objects and notification policies and to learn statuses of your endpoints at any time.

Procedure

1. Log in to the management console.
2. Hover on ☰ to display **Service List** and choose **Management & Governance** > **Cloud Eye**.
3. In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.

4. On the **Alarm Rules** page, click **Create Alarm Rule** to create one. (You can also modify an existing alarm rule.)
5. In the displayed **Create Alarm Rule** page, configure parameters.
6. After configuring the parameters, click **Create**.

   After the alarm rule is created, the system automatically notifies you if an alarm is triggered for your VPC endpoint.

   NOTE

   For more information about VPC Endpoint alarm rules, see **Cloud Eye User Guide**.

4.4 Viewing Metrics

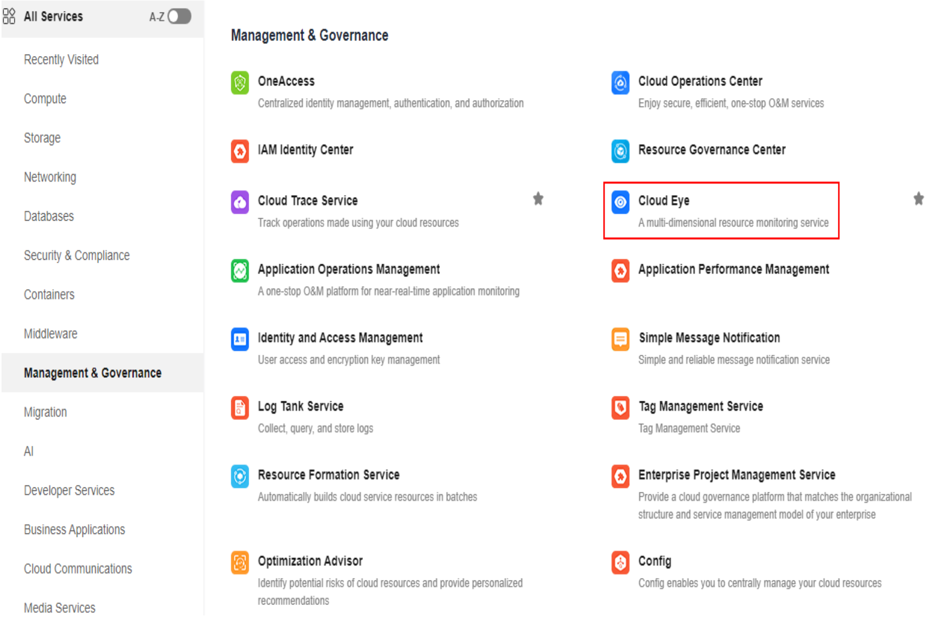
You can view details of VPC Endpoint metrics on the Cloud Eye console.

Procedure

You can perform the same steps as described in the following to view the metrics of a VPC endpoint service or a VPC endpoint.

1. Log in to the management console.
2. Hover on ☰ to display **Service List** and choose **Management & Governance** > **Cloud Eye**.

Figure 4-1 Cloud Eye



Management & Governance

OneAccess
Centralized identity management, authentication, and authorization

Cloud Operations Center
Enjoy secure, efficient, one-stop O&M services

IAM Identity Center

Resource Governance Center

Cloud Trace Service
Track operations made using your cloud resources

Cloud Eye
A multi-dimensional resource monitoring service

Application Operations Management
A one-stop O&M platform for near-real-time application monitoring

Application Performance Management

Identity and Access Management
User access and encryption key management

Simple Message Notification
Simple and reliable message notification service

Log Tank Service
Collect, query, and store logs

Tag Management Service
Tag Management Service

Resource Formation Service
Automatically builds cloud service resources in batches

Enterprise Project Management Service
Provide a cloud governance platform that matches the organizational structure and service management model of your enterprise

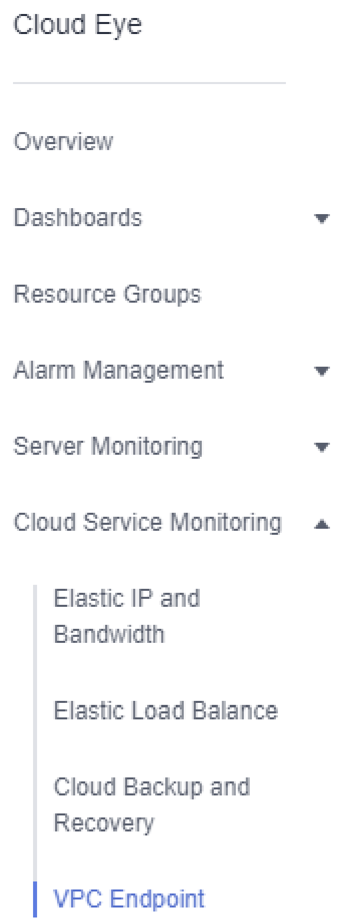
Optimization Advisor
Identify potential risks of cloud resources and provide personalized recommendations

Config
Config enables you to centrally manage your cloud resources

3. In the navigation pane on the left, choose **Cloud Service Monitoring** > **VPC Endpoint**.

   The VPC endpoint service tab is displayed.

Figure 4-2 VPC Endpoint



4. Locate the VPC endpoint service and click **View Metric** in the **Operation** column to view its metrics.

   You can view data of the last 1, 3, 12, or 24 hours, or data of the last 7 days.

5 Using CTS to Audit VPC Endpoints

5.1 Key Operations Recorded by CTS

Scenarios

With Cloud Trace Service (CTS), you can record operations associated with VPC Endpoint for later query, audit, and backtracking.

Prerequisites

You have enabled CTS.

Key VPC Endpoint Operations Recorded by CTS

Table 5-1 VPC Endpoint operations recorded by CTS

Operation	Resource Type	Trace
Creating a VPC endpoint service	EndpointService	createEndpointService
Modifying a VPC endpoint service	EndpointService	modifyEndpointService
Deleting a VPC endpoint service	EndpointService	deleteEndpointService
Rejecting or accepting a VPC endpoint service connection request	EndpointService	serviceConnectionsAction
Adding or removing a whitelist record	EndpointService	servicePermissionAction
Creating a VPC endpoint	vpcEndpoint	createEndpoint

Operation	Resource Type	Trace
Modifying a VPC endpoint	vpcEndpoint	modifyEndpoint
Deleting a VPC endpoint	vpcEndpoint	deleteEndpoint
Modifying routes associated with a VPC endpoint	vpcEndpoint	modifyEndpointRouteTables
Modifying resource tags in batches	vpcEndpointOrService	batchModifyTag

5.2 Viewing Traces

Scenarios

After CTS is enabled, CTS starts recording operations on cloud resources. The CTS management console stores the last seven days of operation records.

This section describes how to query or export the last seven days of operation records on the management console.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. In the upper left corner of the page, click ☰ to go to the service list. Under **Management & Governance**, click **Cloud Trace Service**.
4. In the navigation pane on the left, choose **Trace List**.
5. Specify filters as needed. The following filters are available:
   - **Trace Type**: Set it to **Management** or **Data**.
   - **Trace Source**, **Resource Type**, and **Search By**

     Select filters from the drop-down list.

     If you select **Trace name** for **Search By**, select a trace name.

     If you select **Resource ID** for **Search By**, select or enter a resource ID.

     If you select **Resource name** for **Search By**, select or enter a resource name.
   - **Operator**: Select a specific operator (a user other than an account).
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Search time range: In the upper right corner, choose **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.
6. Click arrow on the left of the required trace to expand its details.

7. Locate the required trace and click **View Trace** in the **Operation** column.

   A dialog box is displayed, showing the trace content.

6 Permissions Management

6.1 Creating a User and Granting VPC Endpoint Permissions

Use **IAM** to implement fine-grained permissions control over your VPC Endpoint resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user has their own security credentials for accessing VPC Endpoint resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust a HUAWEI ID or a cloud service to perform efficient O&M on your VPC Endpoint resources.

If your HUAWEI ID does not need individual IAM users, skip this section.

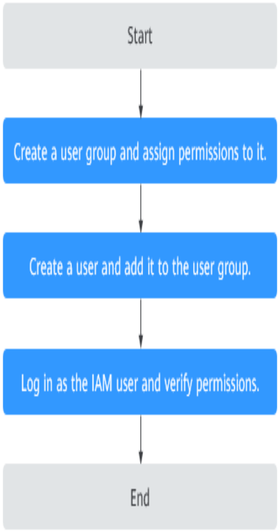
This section describes the process flow for granting permissions (see **Figure 6-1**).

Prerequisites

You must learn about permissions (see **Permissions**) supported by VPC Endpoint and choose policies or roles according to your requirements. To grant permissions for other services, learn about all **System Permissions** supported by IAM.

Process Flow

Figure 6-1 Process for granting VPC Endpoint permissions


Start
Create a user group and assign permissions to it.
Create a user and add it to the user group.
Log in as the IAM user and verify permissions.
End

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

   On the IAM console, create a user group and attach the **VPCEndpoint Administrator** policy to the group.

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

   Create an IAM user and add it to the user group created in **1**.

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

   In the authorized region, perform the following operations:

   - On the **Service List** page, choose **VPC Endpoint**. Click **Buy VPC Endpoint** in the upper right corner. If you can buy a VPC endpoint, the **VPCEndpoint Administrator** policy has already taken effect.
   - Choose another service from **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **VPCEndpoint Administrator** policy has already taken effect.

7 Quotas

What Is Quota?

Quotas can limit the number or amount of resources available to users, such as the maximum number of ECS or EVS disks that can be created.

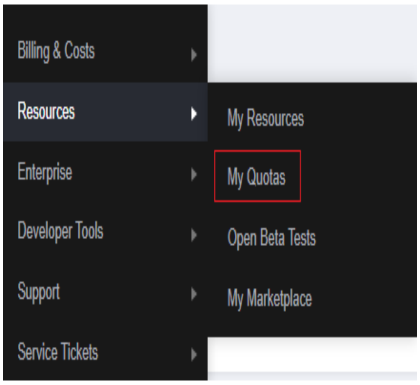
If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources** > **My Quotas**.

   The **Service Quota** page is displayed.

   Figure 7-1 My Quotas

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

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

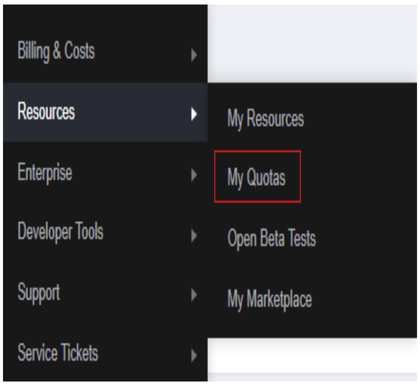
How Do I Apply for a Higher Quota?

1. Log in to the management console.

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

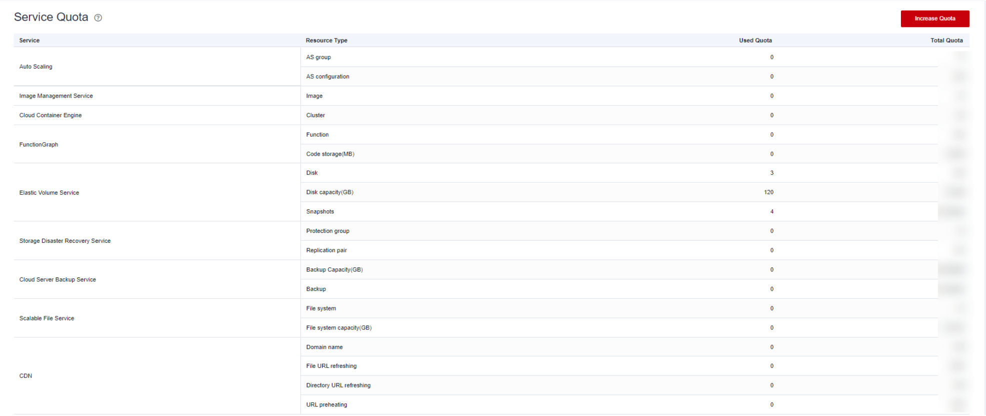
   The **Service Quota** page is displayed.

Figure 7-2 My Quotas



3. Click **Increase Quota** in the upper right corner of the page.

Figure 7-3 Increasing quota



Service Quota

Service	Resource Type	Used Quota	Total Quota
Auto Scaling	AS group	0	[redacted]
	AS configuration	0	[redacted]
Image Management Service	Image	0	[redacted]
Cloud Container Engine	Cluster	0	[redacted]
FunctionGraph	Function	0	[redacted]
	Code storage(MB)	0	[redacted]
Elastic Volume Service	Disk	3	[redacted]
	Disk capacity(GB)	120	[redacted]
	Snapshots	4	[redacted]
Storage Disaster Recovery Service	Protection group	0	[redacted]
	Replication pair	0	[redacted]
Cloud Server Backup Service	Backup Capacity(GB)	0	[redacted]
	Backup	0	[redacted]
Scalable File Service	File system	0	[redacted]
	File system capacity(GB)	0	[redacted]
CDN	Domain name	0	[redacted]
	File URL refreshing	0	[redacted]
	Directory URL refreshing	0	[redacted]
	URL preheating	0	[redacted]

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

   In the **Problem Description** area, fill in the content and reason for adjustment.

5. After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.