VPC Endpoint

User Guide

Issue 01

Date 2026-01-19

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Using IAM to Grant Access to VPC Endpoint

1.1 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.

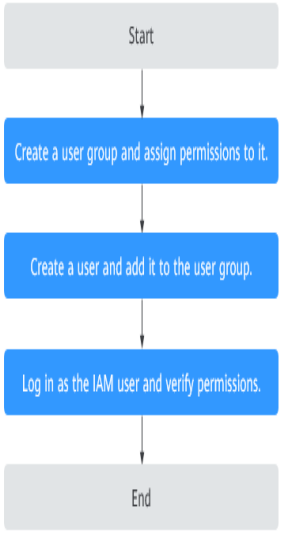
This section describes the process flow for granting permissions (see **Figure 1-1**).

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 1-1 Process for granting VPC Endpoint permissions



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.

2 VPC Endpoint Services

2.1 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 configured by the system only for cloud services.
- Interface VPC endpoint services can be configured for cloud services or private services. Cloud services are configured as interface VPC endpoint services by the O&M personnel by default. However, private services must be configured as interface VPC endpoint services by users.

NOTE

Supported cloud services vary by region. For details, see the services that can be configured on the management console.

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

This section describes how to configure your private service as an interface VPC endpoint service and how to manage it.

Table 2-1 Management of VPC endpoint services

Operation	Description	Constraints
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 as VPC endpoint services: – **Elastic load balancer**: works well for services that need to handle heavy traffic and require strong reliability and effective disaster recovery. – **ECS**: serves as a server. – **BMS**: serves as a server. • A VPC endpoint service can have only one backend resource. • If a Layer 7 load balancer is configured as a backend resource, Proxy Protocol must be disabled.
Managing VPC Endpoint Services	Describes how to check and delete a VPC endpoint service.	• Deleted VPC endpoint services cannot be recovered. • Only private services configured as VPC endpoint services can be deleted. • VPC endpoint services in the **Accepted** or **Creating** state cannot be deleted.
Accepting or Rejecting the Access from a VPC Endpoint	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.

Operation	Description	Constraints
Configuring the Whitelist of a VPC Endpoint Service	Describes how to manage whitelist records of a VPC endpoint service to control cross-account access between a VPC endpoint and a VPC endpoint service.	• The VPC endpoint and 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.
Viewing 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 20 tags to each VPC endpoint service.

2.2 Creating a VPC Endpoint Service

Scenarios

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

- Gateway VPC endpoint services are configured by the system only for cloud services.
- Interface VPC endpoint services can be configured for cloud services or private services. Cloud services are configured as interface VPC endpoint services by the O&M personnel by default. However, private services must be configured as interface VPC endpoint services by users.

This section describes how to configure a private service as 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 as VPC endpoint services:
  - **Elastic load balancer**: works well for services that need to handle heavy traffic and require strong reliability and effective disaster recovery.

  - **ECS**: serves as a server.
  - **BMS**: serves as a server.
- A VPC endpoint service can have only one backend resource.
- If a Layer 7 load balancer is configured as a backend resource, Proxy Protocol must be disabled.

Procedure

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

   The **Create VPC Endpoint Service** page is displayed.
3. Configure parameters by referring to **Table 2-2**.

Table 2-2 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 faster access, select the region nearest to where your services will be accessed.
Name (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.
VPC	Specifies the VPC where the VPC endpoint service is to be deployed.
Service Type	Specifies the type of the VPC endpoint service. The default value is **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 **Accepting or Rejecting the Access from a VPC Endpoint**.

Parameter	Description
Backend Resource Type	Specifies the type of the backend resource that provides services to be accessed. The following backend resource types are supported: • **Elastic load balancer**: works well for services that need to handle heavy traffic and require strong reliability and effective disaster recovery. • **ECS**: serves as a server. • **BMS**: serves as a server. 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**, to allow inbound traffic. 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 there is a rule that allows traffic from 198.19.128.0/17.
Load Balancer	Specifies the load balancer that will provide services. When **Backend Resource Type** is set to **Elastic load balancer**, select a load balancer from the drop-down list. **NOTE** If a load balancer is used as the backend resource, the client IP address cannot be obtained.
ECS	This parameter is available when you select **ECS** for **Backend Resource Type**. Select an ECS from the ECS list.
BMS	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. Use load balancers as backend resources instead.
Port Mapping	Specifies the protocol and ports used for communications between the VPC endpoint service and a VPC endpoint. The protocol can be TCP. • **Service Port**: a port used by the VPC endpoint service to provide services. • **Endpoint Port**: a VPC endpoint port for you to access a VPC endpoint service. The service and endpoint 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 endpoint port.

Parameter	Description
Tag (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 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**.
Description (Optional)	Provides supplementary information about the VPC endpoint service.

Table 2-3 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 128 characters. • Can contain letters, digits, spaces, and any of the following characters: _.:=+-@. It cannot start or end with a space, or start with _sys_.
Tag value	• Can be left blank. • Can contain a maximum of 255 characters. • Can contain letters, digits, spaces, and any of the following characters: _.:=+-@. It cannot start or end with a space.

4. Click **Create Now**.
5. Return to the VPC endpoint service list and check the new VPC endpoint service.

2.3 Managing VPC Endpoint Services

Viewing a VPC Endpoint Service

The following describes how to view the details of a VPC endpoint service.

You can follow the instructions to view the 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.

1. Go to the **VPC endpoint service list** page.
2. In the search box above the VPC endpoint service list, enter the search criteria to quickly locate the VPC endpoint service.

3. Click the name of a VPC endpoint service to view its basic information and configurations.

   Table 2-4 describes the parameters displayed on the VPC endpoint service details page.

Table 2-4 Parameter descriptions

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	Backend Resource Name	Specifies the name of the backend resource that provides services.
Summary	VPC	Specifies the VPC where the VPC endpoint service is 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 Are Statuses of VPC Endpoint Services and VPC Endpoints?**
Connection Management	Owner	Specifies the account ID of the VPC endpoint owner.
Connection Management	Created	Specifies when the VPC endpoint was created.

Tab	Parameter	Description
Connection Management	Operation	Specifies whether to allow a VPC endpoint to access a VPC endpoint service. The option can be **Accept** or **Reject**.
Permission Management	Authorized Account ID	Specifies the authorized account ID for accessing the VPC endpoint service. 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 VPC endpoint.
Port Mapping	Service Port	Specifies the port used by the VPC endpoint service to provide services.
Port Mapping	Endpoint Port	Specifies the VPC endpoint for you to access the VPC endpoint service.
Tags	Key	Specifies the tag key of the VPC endpoint service.
Tags	Value	Specifies the tag value of the VPC endpoint service.
Tags	Edit Tag	Specifies the operation to be performed on the VPC endpoint service tag. You can edit or delete a tag.

Deleting a VPC Endpoint Service

You can delete a VPC endpoint service that is no longer needed. Deleted VPC endpoint services cannot be recovered.

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

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

The following describes how you can delete a VPC endpoint service.

1. Go to the **VPC endpoint service list** page.
2. In the VPC endpoint service list, locate the target endpoint service and click **Delete** in the **Operation** column.
3. In the **Delete This VPC Endpoint Service** dialog box, click **OK**.

2.4 Accepting or Rejecting the Access from a VPC Endpoint

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 the access from a VPC endpoint.

Prerequisites

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

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

2.5 Configuring the Whitelist of a VPC Endpoint Service

Scenarios

You can use a whitelist to control the access from 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 accessing 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 accessing 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 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 VPC endpoint.

Adding 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**.

   NOTE

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

Deleting 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**.

2.6 Viewing Port Mappings of a VPC Endpoint Service

Scenarios

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

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. On the displayed page, select the **Port Mapping** tab.
   The port mappings configured for the VPC endpoint service are displayed.

2.7 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**.

Adding 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.
   Table 2-5 describes the tag requirements.

   Table 2-5 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 128 characters. • Can contain letters, digits, spaces, and any of the following characters: _.:=+-@. It cannot start or end with a space, or start with _sys_.
Tag value	• Can be left blank. • Can contain a maximum of 255 characters. • Can contain letters, digits, spaces, and any of the following characters: _.:=+-@. It cannot start or end with a space.

6. Click **OK**.

Editing 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**.

Deleting 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**.

3 VPC Endpoints

3.1 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.

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

Table 3-1 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 for accessing 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.
Accessing a VPC Endpoint Through Its Private IP Address or Private Domain Name	Describes how to query the summary of a VPC endpoint.	One VPC endpoint supports up to 3,000 concurrent connections.
Managing VPC Endpoints	Describes how to delete a VPC endpoint.	Deleted VPC endpoints cannot be recovered.

Operation	Description	Constraint
Configuring Access Control for an Interface VPC Endpoint	Describes how to enable access control for a VPC endpoint and configure IP addresses and 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 20 tags to each VPC endpoint.

3.2 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 must have 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 work as gateways, with routes configured to distribute traffic to the associated gateway VPC endpoint service.

NOTE

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

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

- **Buying a VPC Endpoint for Accessing an Interface VPC Endpoint Service**
- **Buying a VPC Endpoint for Accessing a Gateway VPC Endpoint Service**

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 for accessing 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 an Interface VPC Endpoint Service

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.

Table 3-2 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 faster access, select the region nearest to where your services will be accessed.
Billing Mode	Specifies the billing mode of the VPC endpoint. You are billed by how long you use each VPC endpoint. VPC endpoints can be used or deleted at any time. Only pay-per-use billing is supported.
Service Category	There are two options: • **Cloud services**: Select it if the target VPC endpoint service is a cloud service. • **Find a service by name**: Select it if the target VPC endpoint service is your private service.
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 the service is found, proceed with subsequent operations. ● If the service is not found, 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	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 deployed.
Access Control	This parameter is available when you want to access an interface VPC endpoint service. You can specify IP addresses and CIDR blocks that are allowed to access the VPC endpoint. ● If **Access Control** is enabled, only IP addresses and CIDR blocks in the whitelist are allowed to access the VPC endpoint. ● If **Access Control** is disabled, any IP address and 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. You can specify the IP addresses and 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.

Parameter	Description
Tag (Optional)	Specifies the tags that are used to classify and identify the VPC endpoint. Each tag 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 3-3**. **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**.
Description (Optional)	Provides supplementary information about the VPC endpoint.

Table 3-3 Tag requirements for VPC endpoints

Parameter	Requirement
Tag key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Can contain letters, digits, spaces, and any of the following characters: _.:=+-@. It cannot start or end with a space, or start with _sys_.
Tag value	• Can be left blank. • Can contain a maximum of 255 characters. • Can contain letters, digits, spaces, and any of the following characters: _.:=+-@. It cannot start or end with a space.

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 a Gateway VPC Endpoint Service

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.

Table 3-4 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 faster access, select the region nearest to where your services will be accessed.
Billing Mode	Specifies the billing mode of the VPC endpoint. You are billed by how long you use each VPC endpoint. VPC endpoints can be used or deleted at any time. Only pay-per-use billing is supported.
Service Category	There are two options: • **Cloud services**: Select it if the target VPC endpoint service is a cloud service. • **Find a service by name**: Select it if the target VPC endpoint service is your private service.
Service List	This parameter is available only when you select **Cloud services** for **Service Category**. In the VPC endpoint service list, select a gateway VPC endpoint service. The VPC endpoint service has been created by the O&M personnel and you can directly use it. **NOTE** To access OBS as a gateway VPC endpoint service, you need to search for it by name. To obtain its name, **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 the service is found, proceed with subsequent operations. • If the service is not found, 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 accessing a gateway VPC endpoint service. **NOTE** This parameter is available only in the regions where the route table function is enabled. You are advised to select all route tables. Otherwise, access may fail. Select the route tables in the VPC where the VPC endpoint is created as required. For details about how to add a route, see **Adding a Custom Route** in the *Virtual Private Cloud User Guide*.
Tag (Optional)	Specifies the tags that are used to classify and identify the VPC endpoint. Each tag 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 3-5**. **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**.
Description (Optional)	Provides supplementary information about the VPC endpoint.

Table 3-5 Tag requirements for VPC endpoints

Parameter	Requirement
Tag key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Can contain letters, digits, spaces, and any of the following characters: _.:=+-@. It cannot start or end with a space, or start with _sys_.
Tag value	• Can be left blank. • Can contain a maximum of 255 characters. • Can contain letters, digits, spaces, and any of the following characters: _.:=+-@. It cannot start or end with a space.

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**.

3.3 Managing VPC Endpoints

Querying a VPC Endpoint

You can query the 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. In the search box above the VPC endpoint list, enter the search criteria as prompted to quickly locate the VPC endpoint.
3. Click the name of a VPC endpoint to view its basic information and configurations.

Table 3-6 Parameter descriptions

Tab	Parameter	Description
Summary	ID	Specifies the ID of the VPC endpoint.
Summary	VPC	Specifies the VPC where the VPC endpoint is deployed.
Summary	VPC Endpoint Service Name	Specifies the name of the VPC endpoint service that the VPC endpoint is used to access.
Summary	Private IP Address	Specifies the IP address of the VPC endpoint.
Summary	Private Domain Name	Specifies the private domain name for accessing the VPC endpoint.
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	Created	Specifies when the VPC endpoint was created.

Tab	Parameter	Description
Summary	Access Control	Specifies whether access control is enabled to use a whitelist to control access to 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	Specifies the 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 accessing interface VPC endpoint services.
Access Control	Operation	Specifies the operation to be performed on whitelist records of the VPC endpoint. Only deletion is supported.
Route Table	Name	Specifies the name of the route table. **NOTE** The **Route Tables** tab is displayed only for the VPC endpoint to access a gateway VPC endpoint service in some specific regions.
Route Table	VPC	Specifies the VPC that the route table belongs to.
Route Table	Type	Specifies the type of the route table, which can be **Default** or **Custom**.
Route Table	Associated Subnets	Specifies the number of subnets associated with the route table.

Tab	Parameter	Description
Route Table	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.
Policy	VPC Endpoint Policy	Specifies a policy to control access from the VPC endpoint to a VPC endpoint service. **NOTE** The **Policy** tab is displayed only for the VPC endpoint to access a gateway VPC endpoint service in some specific regions.
Tags	Key	Specifies the tag key of the VPC endpoint.
Tags	Value	Specifies the tag value of the VPC endpoint.
Tags	Edit Tag	Specifies the operation to be performed on the VPC endpoint tag. You can edit or delete a tag.

Deleting a VPC Endpoint

Deleted VPC endpoints cannot be recovered.

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

3.4 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 configure access control for an existing VPC endpoint.

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.

Enabling Access Control and Adding 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**.
5. Enter the IP addresses and CIDR blocks in the **IP Address or CIDR Block** column.

   NOTE

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

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

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

3.5 Accessing a VPC Endpoint Through Its Private IP Address or Private Domain Name

Scenarios

You can access a VPC endpoint through its private IP address or private domain name.

Constraints

One VPC endpoint supports up to 3,000 concurrent connections.

Accessing a VPC Endpoint Through Its Private IP Address

Perform the following operations to access a VPC endpoint through 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 Through Its Private Domain Name

You can access a VPC endpoint through 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.

1. Check the record set of the private domain name.
   a. Log in to the management console.
   b. Hover the cursor over  in the upper left corner. In the service list, choose **Networking** > **Domain Name Service**.

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

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

      When **Status** changes to **Normal**, the resolution takes effect.
2. Accessing a VPC endpoint through its private domain name.
   a. In the VPC where the VPC endpoint is deployed, log in to the backend resource, for example, an ECS.
   b. 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*

3.6 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**.

Adding 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.

   Table 3-7 describes the tag requirements.

   Table 3-7 Tag requirements for VPC endpoints

Parameter	Requirement
Tag key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Can contain letters, digits, spaces, and any of the following characters: _.:=+-@. It cannot start or end with a space, or start with _sys_.
Tag value	• Can be left blank. • Can contain a maximum of 255 characters. • Can contain letters, digits, spaces, and any of the following characters: _.:=+-@. It cannot start or end with a space.

6. Click **OK**.

Editing 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**.

Deleting 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**.

4 Quota Adjustment

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

