

VPC Endpoint

Getting Started

Issue 01
Date 2025-01-14



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

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

Trademarks and Permissions



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

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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

| | |
|---|-----------|
| 1 Operation Guide..... | 1 |
| 2 Configuring a VPC Endpoint for Communications Across VPCs of the Same Account..... | 2 |
| 2.1 Overview..... | 2 |
| 2.2 Preparations..... | 3 |
| 2.3 Step 1: Create a VPC Endpoint Service..... | 3 |
| 2.4 Step 2: Buy a VPC Endpoint..... | 8 |
| 3 Configuring a VPC Endpoint for Communications Across VPCs of Different Accounts..... | 14 |
| 3.1 Overview..... | 14 |
| 3.2 Preparations..... | 15 |
| 3.3 Step 1: Create a VPC Endpoint Service..... | 16 |
| 3.4 Step 2: Add a Whitelist Record..... | 20 |
| 3.5 Step 3: Buy a VPC Endpoint..... | 22 |
| 4 Configuring a VPC Endpoint for Accessing the Private IP Address of OBS..... | 28 |
| 4.1 Overview..... | 28 |
| 4.2 Preparations..... | 29 |
| 4.3 Step 1: Buy a VPC Endpoint for Connecting to DNS..... | 30 |
| 4.4 Step 2: Buy a VPC Endpoint for Connecting to OBS..... | 33 |
| 4.5 Step 3: Access OBS Using a VPN or Direct Connect Connection..... | 37 |

1 Operation Guide

Application Scenarios

VPC Endpoint can be used in different scenarios. For details, see [Table 1-1](#).

Table 1-1 Application scenarios

| Scenario | Description |
|---|---|
| Communications between cloud resources across VPCs in the same region | You can create a VPC endpoint service and buy a VPC endpoint to access cloud services across VPCs. For details, see the following sections: <ul style="list-style-type: none">• Configuring a VPC Endpoint for Communications Across VPCs of the Same Account• Configuring a VPC Endpoint for Communications Across VPCs of Different Accounts |
| Access to cloud resources from an on-premises data center | VPC Endpoint allows you to access cloud resources from your on-premises data centers. Configuring a VPC Endpoint for Accessing the Private IP Address of OBS |

2 Configuring a VPC Endpoint for Communications Across VPCs of the Same Account

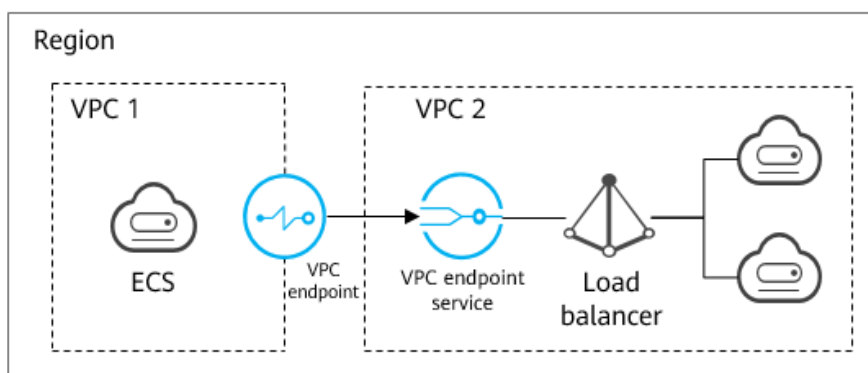
2.1 Overview

With VPC Endpoint, you can access resources across VPCs in the same region.

Cloud resources in different VPCs are isolated from each other and cannot be accessed using private IP addresses. VPC Endpoint enables you to use a private IP address to access resources across two VPCs despite of network isolation between them.

This section describes how cloud resources in VPCs of the same account in the same region can communicate with each other.

As shown in the following figure, VPC 1 and VPC 2 belong to the same account in the same region. You can configure ELB in VPC 2 as a VPC endpoint service and buy a VPC endpoint in VPC 1. Then the ECS in VPC 1 can access ELB in VPC 2 using the private IP address.



 NOTE

- Only one-way communications from the VPC endpoint to the VPC endpoint service are supported.
- For details about communications between two VPCs of different accounts, see [Configuring a VPC Endpoint for Communications Across VPCs of Different Accounts](#).

Required Steps

| What You Need to Do | Description |
|---|---|
| Preparations | Before using the VPC Endpoint service, you need to sign up for a HUAWEI ID, enable Huawei Cloud services, and complete real-name authentication. Also, you need to top up your account. |
| Step 1: Create a VPC Endpoint Service | To enable communications across two VPCs, you first need to configure a cloud resource (backend resource) in one VPC as a VPC endpoint service. |
| Step 2: Buy a VPC Endpoint | After you create a VPC endpoint service, you also need to buy a VPC endpoint to access the VPC endpoint service. |

2.2 Preparations

If you already have a Huawei Cloud account, use it to log in to the VPC Endpoint console. If you do not have a Huawei Cloud account, perform the following operations to sign up:

 NOTE

The VPC Endpoint service is not available on the Huawei Cloud application. You can only use it on the Huawei Cloud management console.

1. Sign up for a HUAWEI ID and complete real-name authentication.
For details, see [Signing up for a HUAWEI ID and Enabling Huawei Cloud Services](#) and [Completing Real-Name Authentication](#).
If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.
2. Top up your account.
Ensure that your account has sufficient balance. For details, see [Topping Up an Account](#).

2.3 Step 1: Create a VPC Endpoint Service

Scenarios

To enable communications across two VPCs, you first need to configure a cloud resource (backend resource) in one VPC as a VPC endpoint service.

This section uses a load balancer as an example to describe how to create a VPC endpoint service.

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 2-1 Create VPC Endpoint Service

The screenshot shows the 'Create VPC Endpoint Service' configuration page. The settings are as follows:

- Region:** A dropdown menu with a search icon.
- Name:** A text input field with the placeholder 'Enter a name.'
- Network Type:** Radio buttons for 'IPv4' (selected) and 'IPv6'.
- VPC:** A dropdown menu with a search icon and a link 'View VPCs'.
- Service Type:** A button labeled 'Interface'.
- Connection Approval:** A toggle switch that is turned on.
- Port Mapping:** A section with 'Protocol' set to 'TCP', 'Service Port' set to '8089', and 'Terminal Port' set to '80'. There are also 'Example' labels for each.
- Backend Resource Type:** Radio buttons for 'Elastic load balancer' (selected), 'ECS', and 'BMS'.
- Load Balancer:** A dropdown menu with a search icon and a link 'View load balancers'.
- Tag:** A section with 'Tag key' and 'Tag value' input fields. A note says 'It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags'.

A 'Create Now' button is located at the bottom right of the form.

3. Configure required parameters.

Table 2-1 Parameters for creating a VPC endpoint service

| Parameter | Example Value | Description |
|-----------|---------------|---|
| Region | CN-Hong Kong | 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. |

| Parameter | Example Value | Description |
|---------------------|---------------|--|
| Name | - | <p>This parameter is optional.</p> <p>Specifies the name of the VPC endpoint service.</p> <p>The name can contain a maximum of 16 characters, including letters, digits, underscores (_), and hyphens (-).</p> <ul style="list-style-type: none">• 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 | IPv4 | <p>Specifies the type of the VPC endpoint service.</p> <p>The value can be IPv4 or IPv6.</p> <ul style="list-style-type: none">• IPv4: Only IPv4 networks are supported.• IPv6: Only IPv6 networks are supported. |
| VPC | - | <p>Specifies the VPC where the VPC endpoint service is to be deployed.</p> |
| Subnet | - | <p>Specifies the subnet where the VPC endpoint service is to be deployed.</p> <p>This parameter is mandatory when you set Network Type to IPv6.</p> |
| Service Type | Interface | <p>Specifies the type of the VPC endpoint service. The type can only be Interface.</p> |
| Connection Approval | - | <p>Specifies whether the connection between a VPC endpoint and a VPC endpoint service requires approval from the owner of the VPC endpoint service.</p> <p>You can enable or disable Connection Approval.</p> <p>When Connection Approval is enabled, any VPC endpoint for connecting to the VPC endpoint service needs to be approved. For details, see step 5.</p> |

| Parameter | Example Value | Description |
|--------------|---------------|---|
| Port Mapping | 80 | <p>Specifies the protocol and ports used for communications between the VPC endpoint service and a VPC endpoint. The protocol is TCP or UDP.</p> <ul style="list-style-type: none">• 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. <p>The service and terminal port numbers range from 1 to 65535. A maximum of 50 port mappings can be added at a time.</p> <p>NOTE Accessing a VPC endpoint service from a VPC endpoint is to access the service port from the associated terminal port. If you need to run an SSH command to verify the connectivity after the configuration is complete, set Service Port to 22 according to the SSH protocol.</p> |

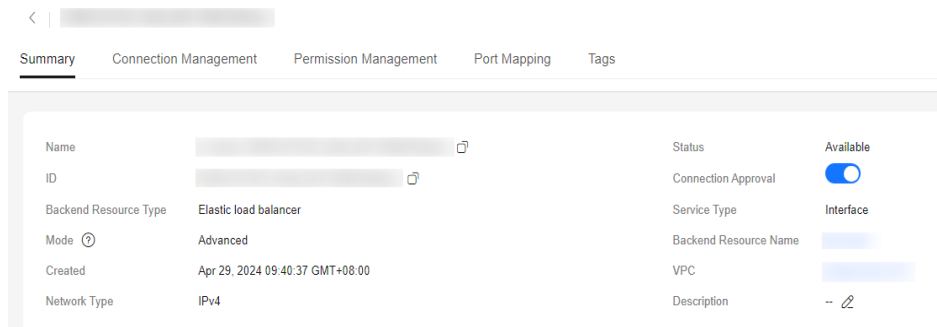
| Parameter | Example Value | Description |
|-----------------------|--------------------------------|---|
| Backend Resource Type | Elastic load balancer | <p>Specifies the backend resource that provides services to be accessed.</p> <p>The following backend resource types are supported:</p> <ul style="list-style-type: none">• 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. <p>In this example, select Elastic load balancer.</p> <p>NOTE</p> <ul style="list-style-type: none">• 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 <i>Virtual Private Cloud User Guide</i>.• 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 | - | <p>When Backend Resource Type is set to Elastic load balancer, select the load balancer that provides services from the drop-down list.</p> <p>NOTE</p> <p>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.</p> |
| Tag | example_key1 example_value1 | <p>Specifies the tag that is used to classify and identify the VPC endpoint service.</p> <p>This parameter can be modified after you create a VPC endpoint service.</p> |

| Parameter | Example Value | Description |
|-------------|---------------|--|
| Description | - | Provides supplementary information about the VPC endpoint service. |

Table 2-2 Tag requirements for VPC endpoint services

| Parameter | Requirement |
|-----------|--|
| Tag key | <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • 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.
6. In the VPC endpoint service list, locate the VPC endpoint service and click its name to view its details.



2.4 Step 2: Buy a VPC Endpoint

Scenarios

After you create a VPC endpoint service, you also need to buy a VPC endpoint to access the VPC endpoint service.

This section describes how to buy a VPC endpoint in another VPC of your own.

NOTE

Select the same region and project as those of the VPC endpoint service.

Procedure

1. Go to the [VPC endpoint list](#) page.
2. On the **VPC Endpoints** page, click **Buy VPC Endpoint**.

The **Buy VPC Endpoint** page is displayed.

< | Buy VPC Endpoint

* Region: [dropdown]

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: [input] | 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 | View VPCs

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

* IPV4 Address: Automatically assign IP address | Manually specify IP address

Access Control:

3. Configure required parameters.

Table 2-3 VPC endpoint parameters

| Parameter | Example Value | Description |
|------------------|------------------------|---|
| Region | CN-Hong Kong | Specifies the region where the VPC endpoint is to be located. This region is the same as that of the VPC endpoint service. |
| Billing Modes | Pay-per-use | 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 | Find a service by name | There are two options: <ul style="list-style-type: none"> • 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. In this example, select Find a service by name . |

| Parameter | Example Value | Description |
|------------------------------|---------------|--|
| VPC Endpoint Service Name | - | <p>This parameter is available only when you select Find a service by name for Service Category.</p> <p>Enter the VPC endpoint service name recorded in 6 and click Verify.</p> <ul style="list-style-type: none">• 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 | - | <p>If you want to access a VPC endpoint using a domain name, select Create a Private Domain Name.</p> <p>This parameter is mandatory when the VPC endpoint will be used to access an interface VPC endpoint service.</p> |
| VPC Endpoint Type | Interface | <p>This parameter is displayed based on the type of the VPC endpoint service to be connected.</p> <ul style="list-style-type: none">• 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 | Professional | <p>This parameter is mandatory when you are going to connect to an interface VPC endpoint service.</p> <p>Professional is selected by default.</p> <p>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.</p> |

| Parameter | Example Value | Description |
|----------------|---------------|---|
| Network Type | IPv4 | <p>This parameter is mandatory when you are going to connecting to an interface VPC endpoint service whose Mode is Advanced.</p> <p>This parameter can be set to IPv4 or Dual stack.</p> <ul style="list-style-type: none">• 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 | - | Specifies the subnet where the VPC endpoint is to be located. |
| IPv4 Address | - | IPv4 addresses can be automatically assigned or manually specified. |
| IPv6 Address | - | <p>This parameter is mandatory when you select Professional for VPC Endpoint Edition and Dual stack for Network Type.</p> <p>IPv6 addresses can be automatically assigned or manually specified.</p> |
| Access Control | Enable | <p>This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service.</p> <p>It controls IP addresses and CIDR blocks that are allowed to access the VPC endpoint.</p> <ul style="list-style-type: none">• 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 | - | <p>This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service.</p> <p>It lists the IP addresses or CIDR blocks that are allowed to access the VPC endpoint. You can add a maximum of 20 records.</p> |

| Parameter | Example Value | Description |
|-------------|--------------------------------|--|
| 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 | example_key1 example_value1 | Specifies the tag that is used to classify and identify the VPC endpoint. This parameter can be modified after you buy a VPC endpoint. |
| Description | - | Provides supplementary information about the VPC endpoint. |

Table 2-4 Tag requirements for VPC endpoints

| Parameter | Requirement |
|-----------|---|
| Tag key | <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• Cannot be left blank.• Can contain a maximum of 43 characters.• Can contain only letters, digits, hyphens (-), and underscores (_). |

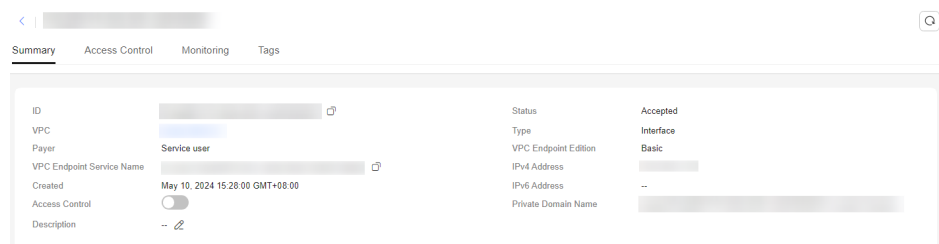
4. Confirm the settings and click **Next**.
 - If all of the settings are correct, click **Submit**.
 - If any of the settings are incorrect, click **Previous** to modify the parameter settings as needed, and click **Submit**.
5. Manage the connection of the VPC endpoint.

If the status of the VPC endpoint changes to **Accepted**, the VPC endpoint is connected to the required VPC endpoint service. If the status is **Pending acceptance**, connection approval is enabled for the VPC endpoint service, ask the owner of the VPC endpoint service to perform the following operations:

- a. Locate the VPC endpoint service and click its name.
- b. On the displayed page, select the **Connection Management** tab.

- If you allow a VPC endpoint to connect to this VPC endpoint service, locate the VPC endpoint and click **Accept** in the **Operation** column.
 - If you do not allow a VPC endpoint to connect to this VPC endpoint service, click **Reject** in the **Operation** column.
- c. Go back to the VPC endpoint list and check whether the status of the target VPC endpoint changes to **Accepted**. If yes, the VPC endpoint is connected to the VPC endpoint service.
6. In the VPC endpoint list, click the ID of the target VPC endpoint to view its details.

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



You can use the private IP address or private domain name to access the VPC endpoint service.

Configuration Verification

Remotely log in to an ECS in VPC 1 by running an SSH command and access the private IP address or private domain name of the VPC endpoint, as shown in the following figure.

```
ssh -p Terminal port IP address of the VPC endpoint
```



CAUTION

According to the SSH protocol, set the service port to 22 when **creating a VPC endpoint service**. Or, the SSH command cannot be used for verification.

```
Last login: Tue Sep 12 09:44:50 2023 from 10.0.0.231
[root@ ~]# ssh -p 50 172.17.0.149
The authenticity of host '[172.17.0.149]:50 ([172.17.0.149]:50)' can't be established.
ECDSA key fingerprint is SHA256:4P81iW6CBbsNE0P09tI02M4pBaPigH8yjN+r54FuXIY.
No matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```


3 Configuring a VPC Endpoint for Communications Across VPCs of Different Accounts

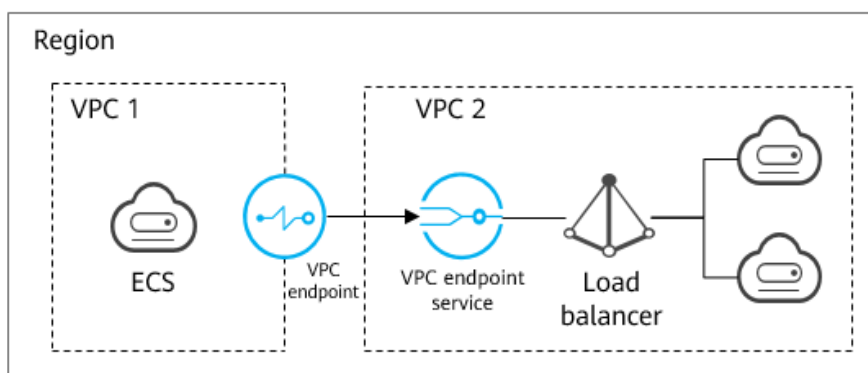
3.1 Overview

With VPC Endpoint, you can access resources across VPCs in the same region.

Cloud resources in different VPCs are isolated from each other and cannot be accessed using private IP addresses. VPC Endpoint enables you to use a private IP address to access resources across two VPCs despite of network isolation between them.

This section describes how cloud resources in VPCs of different accounts in the same region can communicate with each other.

As shown in the following figure, VPC 1 and VPC 2 belong to different accounts. You can configure ELB in VPC 2 as a VPC endpoint service and buy a VPC endpoint in VPC 1 so that the ECS in VPC 1 can access ELB in VPC 2 using a private IP address.



 NOTE

- Only one-way communications from the VPC endpoint to the VPC endpoint service are supported.
- Before you buy a VPC endpoint, add the authorized account ID of VPC 1 to the whitelist of the VPC endpoint service in VPC 2.
- For details about communications between two VPCs of the same account, see [Configuring a VPC Endpoint for Communications Across VPCs of the Same Account](#).

Required Steps

| What You Need to Do | Description |
|---|---|
| Preparations | Before using the VPC Endpoint service, you need to sign up for a HUAWEI ID, enable Huawei Cloud services, and complete real-name authentication. Also, you need to top up your account. |
| Step 1: Create a VPC Endpoint Service | To enable communications across two VPCs, you first need to configure a cloud resource (backend resource) in one VPC as a VPC endpoint service. |
| Step 2: Add a Whitelist Record | After you create a VPC endpoint service, you also need to buy a VPC endpoint to access the VPC endpoint service. |
| Step 3: Buy a VPC Endpoint | After you add the required whitelist record, you can buy a VPC endpoint in VPC 1 to connect to the target VPC endpoint service. |

3.2 Preparations

If you already have a Huawei Cloud account, use it to log in to the VPC Endpoint console. If you do not have a Huawei Cloud account, perform the following operations to sign up:

 NOTE

The VPC Endpoint service is not available on the Huawei Cloud application. You can only use it on the Huawei Cloud management console.

1. Sign up for a HUAWEI ID and complete real-name authentication.

For details, see [Signing up for a HUAWEI ID and Enabling Huawei Cloud Services](#) and [Completing Real-Name Authentication](#).

If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.

2. Top up your account.

Ensure that your account has sufficient balance. For details, see [Topping Up an Account](#).

3.3 Step 1: Create a VPC Endpoint Service

Scenarios

To enable communications across two VPCs, you first need to configure a cloud resource (backend resource) in one VPC as a VPC endpoint service.

This section describes how to create a VPC endpoint service by selecting an elastic load balancer as an example backend service in VPC 2 using account B.

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 3-1 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:

* Network Type: IPv4 IPv6

* VPC: [View VPCs](#)

* Service Type: Interface

Connection Approval: ⓘ

* Port Mapping: Protocol: Service Port: Terminal Port:

⊕ Add Port Mapping You can add 49 more port mappings.

* Backend Resource Type: Elastic load balancer ECS BMS

* Load Balancer: [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](#) ⓘ

You can add 20 more tags.

[Create Now](#)

3. Configure required parameters.

Table 3-1 Parameters for creating a VPC endpoint service

| Parameter | Example Value | Description |
|--------------|---------------|--|
| Region | CN-Hong Kong | 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 (-). <ul style="list-style-type: none">• 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 | IPv4 | Specifies the type of the VPC endpoint service. The value can be IPv4 or IPv6 . <ul style="list-style-type: none">• 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 set Network Type to IPv6 . |
| Service Type | Interface | Specifies the type of the VPC endpoint service. The type can only be Interface . |

| Parameter | Example Value | Description |
|---------------------|---------------|---|
| Connection Approval | - | <p>Specifies whether the connection between a VPC endpoint and a VPC endpoint service requires approval from the owner of the VPC endpoint service.</p> <p>You can enable or disable Connection Approval.</p> <p>When Connection Approval is enabled, any VPC endpoint for connecting to the VPC endpoint service needs to be approved. For details, see step 5.</p> |
| Port Mapping | 80 | <p>Specifies the protocol and ports used for communications between the VPC endpoint service and a VPC endpoint. The protocol is TCP or UDP.</p> <ul style="list-style-type: none">• 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. <p>The service and terminal port numbers range from 1 to 65535. A maximum of 50 port mappings can be added at a time.</p> <p>NOTE</p> <p>Accessing a VPC endpoint service from a VPC endpoint is to access the service port from the associated terminal port.</p> <p>If you need to run an SSH command to verify the connectivity after the configuration is complete, set Service Port to 22 according to the SSH protocol.</p> |

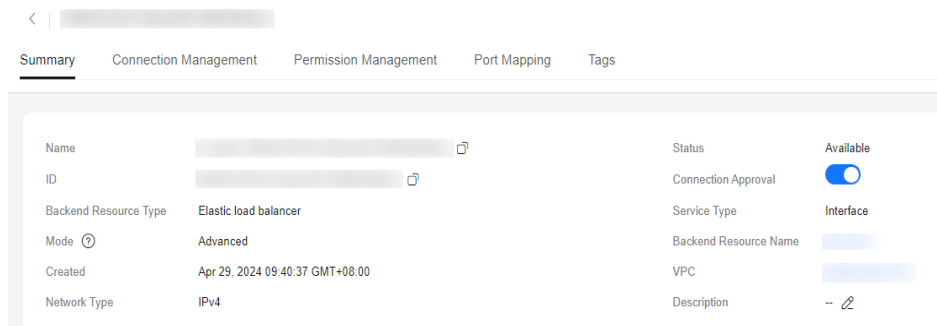
| Parameter | Example Value | Description |
|-----------------------|--------------------------------|--|
| Backend Resource Type | Elastic load balancer | <p>Specifies the backend resource that provides services to be accessed.</p> <p>The following backend resource types are supported:</p> <ul style="list-style-type: none"> • 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. <p>In this example, select Elastic load balancer.</p> <p>NOTE</p> <ul style="list-style-type: none"> • 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 <i>Virtual Private Cloud User Guide</i>. • 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 | - | <p>When Backend Resource Type is set to Elastic load balancer, select the load balancer that provides services from the drop-down list.</p> <p>NOTE</p> <p>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.</p> |
| Tag | example_key1 example_value1 | <p>Specifies the tag that is used to classify and identify the VPC endpoint service.</p> <p>This parameter can be modified after you create a VPC endpoint service.</p> |

| Parameter | Example Value | Description |
|-------------|---------------|--|
| Description | - | Provides supplementary information about the VPC endpoint service. |

Table 3-2 Tag requirements for VPC endpoint services

| Parameter | Requirement |
|-----------|--|
| Tag key | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> Cannot be left blank. Can contain a maximum of 43 characters. Can contain only letters, digits, hyphens (-), and underscores (_). |

- Click **Create Now**.
- Click **Back to VPC Endpoint Service List** to view the newly-created VPC endpoint service.
- In the VPC endpoint service list, locate the VPC endpoint service and click its name to view its details.



3.4 Step 2: Add a Whitelist Record

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.

The following operations describe how to obtain your account ID and add it to the whitelist of another user's VPC endpoint services.

Prerequisites

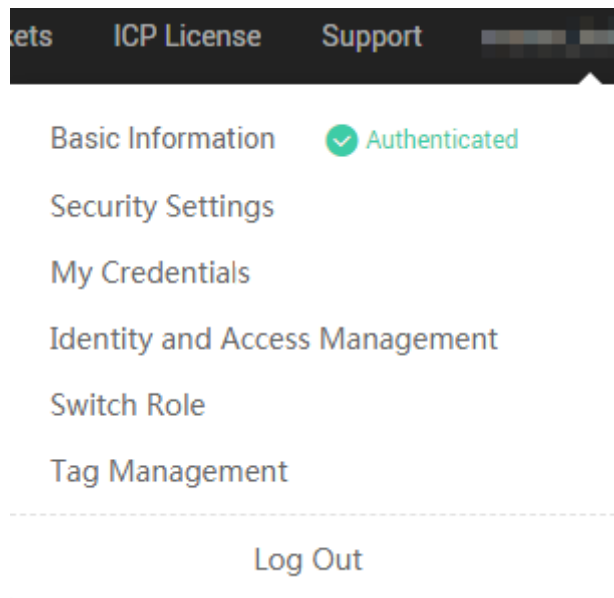
The required VPC endpoint service is available.

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.

Obtain the ID of Your Own Account

1. Log in to the management console.
2. Click **My Credentials** under the account.



The **My Credentials** page is displayed. You can view the account ID of VPC 1.

Figure 3-2 ID

| | | |
|-----------------------------|--|------------------------|
| Username | Tracy110 | |
| User ID | b7a8d7c815604bcaa3dc790a52ea9617 | |
| Account Name | Tracy110 | |
| Account ID | 9b38ce4b05a141c48fd0efde49dd711a | |
| Verified Email Address | No email bound | Bind |
| Mobile Number | +86 136*****98 | Change |
| Password Strength | <div style="width: 100%; height: 10px; background-color: green;"></div> Strong | Change |
| Login Authentication Method | Disable | Change |
| Virtual MFA Device | ! Unbound Bind | |

Add Account IDs to Be Authorized to the Whitelist of a VPC Endpoint Service

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

Add to Whitelist ×

VPC Endpoint Service Name

Add Authorized Account ?

| Authorized Account ID | Operation |
|-----------------------------------|-----------|
| iam:domain:: <input type="text"/> | 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.

3.5 Step 3: Buy a VPC Endpoint

Scenarios

After you add the required whitelist record, you can buy a VPC endpoint in VPC 1 to connect to the target VPC endpoint service.

NOTE

Select the same region and project as those of the VPC endpoint service.

Procedure

1. Go to the [VPC endpoint list](#) page.
2. On the **VPC Endpoints** page, click **Buy VPC Endpoint**.
The **Buy VPC Endpoint** page is displayed.

< | Buy VPC Endpoint ⓘ

* Region: [Region dropdown]

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: [Service Name input] | 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 dropdown] | View VPCs

* Subnet: [Subnet dropdown] | View Subnets | Available IP Addresses: --

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

Access Control: ⓘ

3. Configure required parameters.

Table 3-3 VPC endpoint parameters

| Parameter | Example Value | Description |
|------------------|------------------------|--|
| Region | CN-Hong Kong | Specifies the region where the VPC endpoint is to be located. This region is the same as that of the VPC endpoint service. |
| Billing Modes | Pay-per-use | 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 | Find a service by name | There are two options: <ul style="list-style-type: none">● 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. In this example, select Find a service by name . |

| Parameter | Example Value | Description |
|------------------------------|---------------|---|
| VPC Endpoint Service Name | - | <p>This parameter is available only when you select Find a service by name for Service Category.</p> <p>Enter the VPC endpoint service name recorded in 6 and click Verify.</p> <ul style="list-style-type: none">• 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 | - | <p>If you want to access a VPC endpoint using a domain name, select Create a Private Domain Name.</p> <p>This parameter is mandatory when the VPC endpoint will be used to access an interface VPC endpoint service.</p> |
| VPC Endpoint Type | Interface | <p>This parameter is displayed based on the type of the VPC endpoint service to be connected.</p> <ul style="list-style-type: none">• 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 | Professional | <p>This parameter is mandatory when you are going to connect to an interface VPC endpoint service.</p> <p>Professional is selected by default.</p> <p>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.</p> |

| Parameter | Example Value | Description |
|----------------|---------------|---|
| Network Type | IPv4 | <p>This parameter is mandatory when you are going to connecting to an interface VPC endpoint service whose Mode is Advanced.</p> <p>This parameter can be set to IPv4 or Dual stack.</p> <ul style="list-style-type: none">• 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 | - | Specifies the subnet where the VPC endpoint is to be located. |
| IPv4 Address | - | IPv4 addresses can be automatically assigned or manually specified. |
| IPv6 Address | - | <p>This parameter is mandatory when you select Professional for VPC Endpoint Edition and Dual stack for Network Type.</p> <p>IPv6 addresses can be automatically assigned or manually specified.</p> |
| Access Control | Enable | <p>This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service.</p> <p>It controls IP addresses and CIDR blocks that are allowed to access the VPC endpoint.</p> <ul style="list-style-type: none">• 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 | - | <p>This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service.</p> <p>It lists the IP addresses or CIDR blocks that are allowed to access the VPC endpoint. You can add a maximum of 20 records.</p> |

| Parameter | Example Value | Description |
|-------------|--------------------------------|--|
| 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 | example_key1 example_value1 | Specifies the tag that is used to classify and identify the VPC endpoint. This parameter can be modified after you buy a VPC endpoint. |
| Description | - | Provides supplementary information about the VPC endpoint. |

Table 3-4 Tag requirements for VPC endpoints

| Parameter | Requirement |
|-----------|---|
| Tag key | <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• Cannot be left blank.• Can contain a maximum of 43 characters.• Can contain only letters, digits, hyphens (-), and underscores (_). |

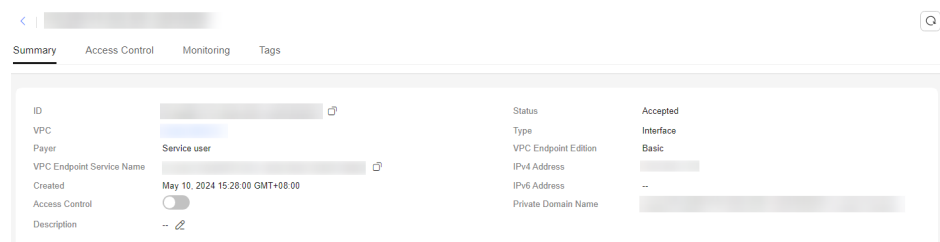
4. Confirm the settings and click **Next**.
 - If all of the settings are correct, click **Submit**.
 - If any of the settings are incorrect, click **Previous** to modify the parameter settings as needed, and click **Submit**.
5. Manage the connection of the VPC endpoint.

If the status of the VPC endpoint changes to **Accepted**, the VPC endpoint is connected to the required VPC endpoint service. If the status is **Pending acceptance**, connection approval is enabled for the VPC endpoint service, ask the owner of the VPC endpoint service to perform the following operations:

- a. Locate the VPC endpoint service and click its name.
- b. On the displayed page, select the **Connection Management** tab.

- If you allow a VPC endpoint to connect to this VPC endpoint service, locate the VPC endpoint and click **Accept** in the **Operation** column.
 - If you do not allow a VPC endpoint to connect to this VPC endpoint service, click **Reject** in the **Operation** column.
- c. Go back to the VPC endpoint list and check whether the status of the target VPC endpoint changes to **Accepted**. If yes, the VPC endpoint is connected to the VPC endpoint service.
6. In the VPC endpoint list, click the ID of the target VPC endpoint to view its details.

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



You can use the private IP address or private domain name to access the VPC endpoint service.

4 Configuring a VPC Endpoint for Accessing the Private IP Address of OBS

4.1 Overview

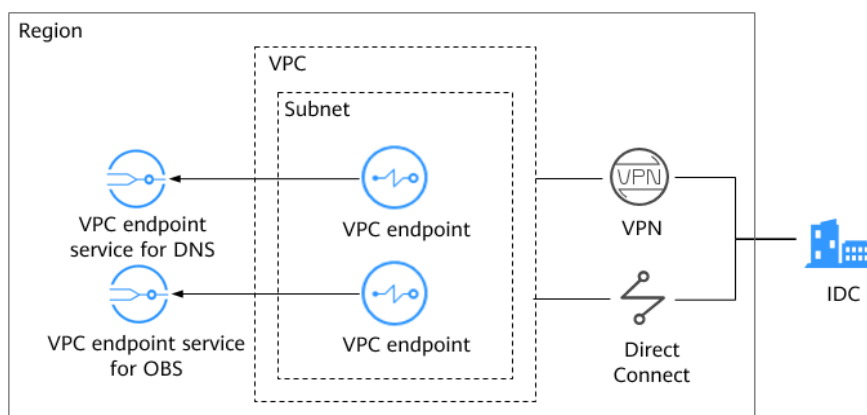
If you want to access a cloud service like OBS from an on-premises data center through an intranet, you can connect the on-premises data center to your VPC using a VPN connection or a Direct Connect connection, and then use a VPC endpoint to access the cloud service from your VPC.

This section describes how to use a VPC endpoint to access OBS (private address) from an on-premises data center.

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. Therefore, this use case is applicable only to these regions.

To access the OBS that is a gateway VPC endpoint service 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.



The preceding figure shows the process of connecting the on-premises data center to a VPC over VPN or Direct Connect, and then using two VPC endpoints to enable the on-premises data center to access DNS and OBS through an intranet.

A VPC endpoint comes with a VPC endpoint service. Before you buy a VPC endpoint, ensure that the VPC endpoint service that you want to access is available.

In this scenario, the following VPC endpoint services are required:

- VPC endpoint service for DNS: required to resolve the OBS domain name.
LA-Mexico City1: **com.myhuaweicloud.na-mexico-1.dns**
- VPC endpoint service for OBS: required to allow the on-premises data center to access the OBS through an intranet.
LA-Mexico City1: **com.myhuaweicloud.na-mexico-1.obs**

Procedure

| Step | Description |
|--|---|
| Preparations | Before using the VPC Endpoint service, you need to sign up for a HUAWEI ID, enable Huawei Cloud services, and complete real-name authentication. Also, you need to top up your account. |
| Step 1: Buy a VPC Endpoint for Connecting to DNS | Buy a VPC endpoint for accessing DNS to resolve the OBS domain name. |
| Step 2: Buy a VPC Endpoint for Connecting to OBS | Buy a VPC endpoint to access OBS from the on-premises data center. |
| Step 3: Access OBS Using a VPN or Direct Connect Connection | Access the OBS through a VPN or Direct Connect connection. |

4.2 Preparations

If you already have a Huawei Cloud account, use it to log in to the VPC Endpoint console. If you do not have a Huawei Cloud account, perform the following operations to sign up:

NOTE

The VPC Endpoint service is not available on the Huawei Cloud application. You can only use it on the Huawei Cloud management console.

1. Sign up for a HUAWEI ID and complete real-name authentication.
For details, see [Signing up for a HUAWEI ID and Enabling Huawei Cloud Services](#) and [Completing Real-Name Authentication](#).

If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.

2. Top up your account.
Ensure that your account has sufficient balance. For details, see [Topping Up an Account](#).

4.3 Step 1: Buy a VPC Endpoint for Connecting to DNS

Scenarios

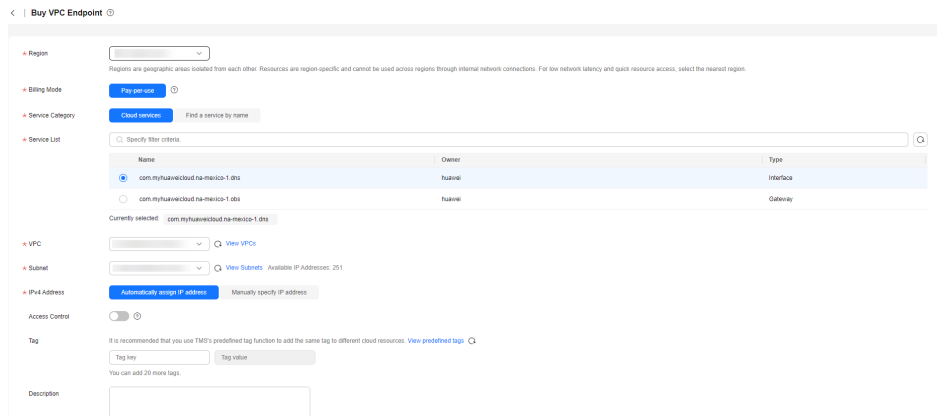
This section describes how to buy a VPC endpoint for accessing DNS to resolve OBS domain names.

Prerequisites

The required VPC endpoint service is available.

Procedure

1. Go to the [VPC endpoint list](#) page.
2. On the **VPC Endpoints** page, click **Buy VPC Endpoint**.
The **Buy VPC Endpoint** page is displayed.



3. Configure VPC endpoint parameters.

Table 4-1 VPC endpoint parameters

| Parameter | Example Value | Description |
|-----------|---------------|---|
| Region | CN-Hong Kong | 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. |

| Parameter | Example Value | Description |
|------------------------------|--|--|
| Billing Mode | Pay-per-use | Specifies the billing mode of the VPC endpoint. Only pay-per-use billing is supported. |
| Service Category | Cloud services | There are two options: <ul style="list-style-type: none">• 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. In this example, select Cloud services . |
| Service List | com.myhuaweicloud.na-mexico-1.dns - | 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 can be directly selected. In this example, select com.myhuaweicloud.na-mexico-1.dns . |
| 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 only when you create a VPC endpoint for connecting to an interface VPC endpoint service. Specifies the subnet where the VPC endpoint is to be located. |

| Parameter | Example Value | Description |
|----------------|--------------------------------|---|
| Access Control | Enable | <p>This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service.</p> <p>It controls IP addresses and CIDR blocks that are allowed to access the VPC endpoint.</p> <ul style="list-style-type: none">• 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 | - | <p>This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service.</p> <p>It lists the IP addresses or CIDR blocks that are allowed to access the VPC endpoint. You can add a maximum of 20 records.</p> |
| Policy | - | <p>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.</p> |
| Tag | example_key1 example_value1 | <p>Specifies the tag that is used to classify and identify the VPC endpoint.</p> <p>The tag settings can be modified after the VPC endpoint is purchased</p> |
| Description | - | <p>Provides supplementary information about the VPC endpoint.</p> |

Table 4-2 Tag requirements for VPC endpoints

| Parameter | Requirement |
|-----------|---|
| Tag key | <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• Cannot be left blank.• Can contain a maximum of 43 characters.• Can contain only letters, digits, hyphens (-), and underscores (_). |

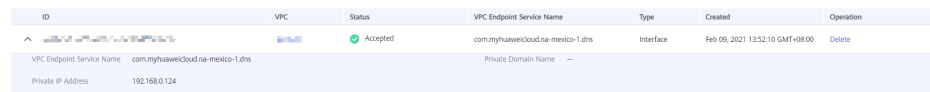
4. Confirm the settings and click **Next**.
 - If all of the settings are correct, click **Submit**.
 - If any of the settings are incorrect, click **Previous** to modify the parameter settings as needed, and click **Submit**.

5. Click **Back to VPC Endpoint List** after the task is submitted.

If the status of the VPC endpoint changes to **Accepted**, the VPC endpoint for connecting to **com.myhuaweicloud.na-mexico-1.dns** is created.

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

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



| ID | VPC | Status | VPC Endpoint Service Name | Type | Created | Operation |
|-----------------------------------|-------------------------------|----------|-----------------------------------|-----------|---------------------------------|-----------|
| com.myhuaweicloud.na-mexico-1.dns | com.myhuaweicloud.na-mexico-1 | Accepted | com.myhuaweicloud.na-mexico-1.dns | Interface | Feb 09, 2021 13:52:10 GMT+08:00 | Delete |

VPC Endpoint Service Name: com.myhuaweicloud.na-mexico-1.dns
Private Domain Name: --
Private IP Address: 192.168.0.124

4.4 Step 2: Buy a VPC Endpoint for Connecting to OBS

Scenarios

This section describes how you can buy a VPC endpoint to securely access OBS from an on-premises data center through an intranet.

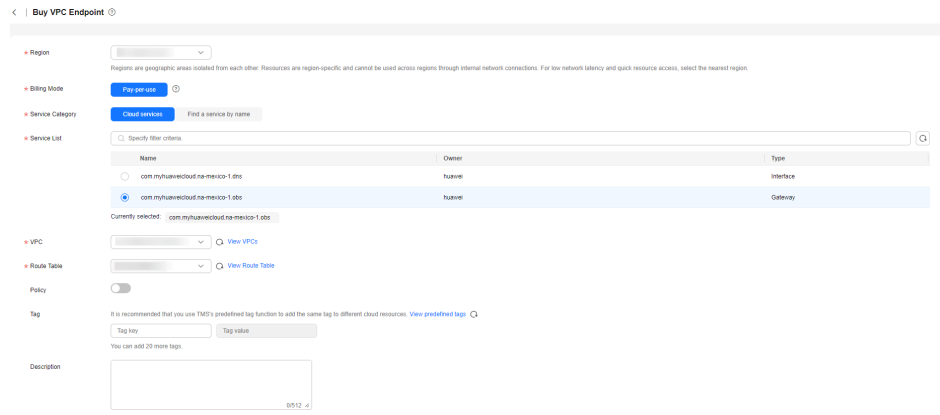
Prerequisites

The required VPC endpoint service is available.

Procedure

1. Go to the [VPC endpoint list](#) page.

2. On the **VPC Endpoints** page, click **Buy VPC Endpoint**.
The **Buy VPC Endpoint** page is displayed.



3. Configure VPC endpoint parameters.

Table 4-3 VPC endpoint parameters

| Parameter | Example Value | Description |
|------------------|----------------|---|
| Region | CN-Hong Kong | 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 | Pay-per-use | Specifies the billing mode of the VPC endpoint. Only pay-per-use billing is supported. |
| Service Category | Cloud services | There are two options: <ul style="list-style-type: none"> • Cloud services: Select this value if the VPC endpoint service to be accessed is a cloud service. • Find a service by name: Select this value if the VPC endpoint service to be accessed is a private service of your own. In this example, select Cloud services . |

| Parameter | Example Value | Description |
|--------------|---------------|---|
| Service List | - | <p>This parameter is available only when you select Cloud services for Service Category.</p> <p>The VPC endpoint service has been created by the O&M personnel and can be directly selected.</p> <p>Select the VPC endpoint service for OBS by region:</p> <ul style="list-style-type: none"> • 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 <p>In this example, select com.myhuaweicloud.na-mexico-1.obs in the LA-Mexico City1 region.</p> |
| VPC | - | Specifies the VPC where the VPC endpoint is to be deployed. |
| Route Table | - | <p>This parameter is available only when you create a VPC endpoint for connecting to a gateway VPC endpoint service.</p> <p>NOTE</p> <p>This parameter is available only in the regions where the route table function is enabled.</p> <p>You are advised to select all route tables. Otherwise, the access to the gateway VPC endpoint service may fail.</p> <p>Select a route table in the VPC where the VPC endpoint will be created.</p> <p>For details about how to add a route, see Adding a Custom Route in the <i>Virtual Private Cloud User Guide</i>.</p> |

| Parameter | Example Value | Description |
|-------------|--------------------------------|--|
| 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 | example_key1 example_value1 | Specifies the tag that is used to classify and identify the VPC endpoint. The tag settings can be modified after the VPC endpoint is purchased. |
| Description | - | Provides supplementary information about the VPC endpoint. |

Table 4-4 Tag requirements for VPC endpoints

| Parameter | Requirement |
|-----------|---|
| Tag key | <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• 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**.
5. Click **Back to VPC Endpoint List** after the task is submitted.

If the status of the VPC endpoint changes from **Creating** to **Accepted**, the VPC endpoint for connecting to **com.myhuaweicloud.na-mexico-1.obs** is created.
6. In the VPC endpoint list, click the ID of the target VPC endpoint to view its details.

4.5 Step 3: Access OBS Using a VPN or Direct Connect Connection

Scenarios

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

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. In the VPC endpoint list, locate the VPC endpoint and click the ID of the endpoint to view its private IP address.
2. 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` is the VPC endpoint's private IP address obtained in 1.
3. Add a route destined for DNS over the VPN gateway or Direct Connect virtual gateway.

To access DNS over a VPN or Direct Connect connection, ensure that traffic from your on-premises data center to DNS is directed to the VPN gateway or Direct Connect gateway.

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 DNS. The following is the example command for configuring such a route:

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

NOTE

- `xx.xx.xx.xx` is the VPC endpoint's private IP address obtained in 1.
 - `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 in the actual OS.
4. Add a route destined for OBS over the VPN gateway or Direct Connect virtual gateway.

The CIDR block of the VPC endpoint for accessing OBS is 100.125.0.0/16. To access OBS over a VPN or Direct Connect connection, ensure that traffic from your on-premises data center to OBS is directed to the VPN gateway or Direct Connect gateway.

Configure a permanent route at your on-premises data center and specify the Direct Connect or VPN gateway as the next hop for accessing OBS. The following is the example command for configuring such a route:

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

NOTE

- `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.
5. At the on-premises data center, run the following command to verify the connectivity with OBS:

```
telnet bucketname.endpoint Port number
```

bucketname.endpoint indicates the domain name of the OBS bucket. You can obtain the domain name by viewing the bucket information on OBS console. For details, see [Viewing Basic Information of a Bucket](#).

In the command:

- *bucketname*: indicates the bucket name.
- *endpoint*: indicates the bucket endpoint (domain name) in the region where the bucket is deployed.
- *Port number*: indicates the service port number, which can be 80 or 443.

Example: **telnet bucketname.obs.na-mexico-1.myhuaweicloud.com 80** or **telnet bucketname.obs.na-mexico-1.myhuaweicloud.com 443**

 NOTE

You can obtain OBS endpoint information at [Regions and Endpoints](#).