VPC Endpoint

Getting Started

Issue 02

Date 2022-01-30



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2022. All rights reserved.

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

Trademarks and Permissions


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

Notice

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

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

Contents

1 Operation Guide..... 1
2 Preparations..... 2
3 Configuring a VPC Endpoint for Communications Across VPCs of the Same Account..... 3
3.1 Overview..... 3
3.2 Step 1: Create a VPC Endpoint Service..... 4
3.3 Step 2: Buy a VPC Endpoint..... 8
4 Configuring a VPC Endpoint for Communications Across VPCs of Different Accounts..... 13
4.1 Overview..... 13
4.2 Step 1: Create a VPC Endpoint Service..... 14
4.3 Step 2: Add a Whitelist Record..... 18
4.4 Step 3: Buy a VPC Endpoint..... 19
5 Configuring a VPC Endpoint for Accessing OBS Using the OBS Private Address..... 24
5.1 Overview..... 24
5.2 Step 1: Buy a VPC Endpoint for Connecting to DNS..... 25
5.3 Step 2: Buy a VPC Endpoint for Connecting to OBS..... 29
5.4 Step 3: Access OBS..... 31
6 Change History..... 34

 Copyright © Huawei Technologies Co., Ltd.

1 Operation Guide

This section uses examples to describe how to use VPCEP.

You can use VPCEP on the VPCEP console. For more information, see **What Is VPC Endpoint?**

Application Scenarios

VPCEP is a perfect fit 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 buy a VPC endpoint service and a VPC endpoint to access cloud services across VPCs. For details, see the following sections: • **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	VPCEP allows you to access cloud resources from your local data center. For details, see the following sections: **Configuring a VPC Endpoint for Accessing OBS Using the OBS Private Address**

 Copyright © Huawei Technologies Co., Ltd.

2 Preparations

Before you use the VPCEP service, make the following preparations:

- **Register with HUAWEI CLOUD and Complete Real-Name Authentication**
- **Top Up Your Account**

Register with HUAWEI CLOUD and Complete Real-Name Authentication

If you already have an authenticated HUAWEI CLOUD account, use it to log in to the VPCEP console. If you do not have a HUAWEI CLOUD account, perform the following operations to register one:

NOTE

The VPCEP service is not available on the HUAWEI CLOUD app. You can only use it on the HUAWEI CLOUD management console.

1. Visit **HUAWEI CLOUD official website**.
2. Click **Register**.

   Enter the required information. For details, see **Registering with HUAWEI CLOUD**.

   After your registration is successful, the system automatically redirects you to your personal information page.
3. Complete real-name authentication for your account. For details, see **Individual Real-Name Authentication**.

Your account has permissions to access the VPCEP service and all other HUAWEI CLOUD services.

Top Up Your Account

Top up your account to ensure that your account has sufficient balance.

- For details about prices and billing rules of VPCEP resources, see **Billing**.
- For details about how to top up an account, see **Topping Up an Account**.

 Copyright © Huawei Technologies Co., Ltd.

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

3.1 Overview

Scenarios

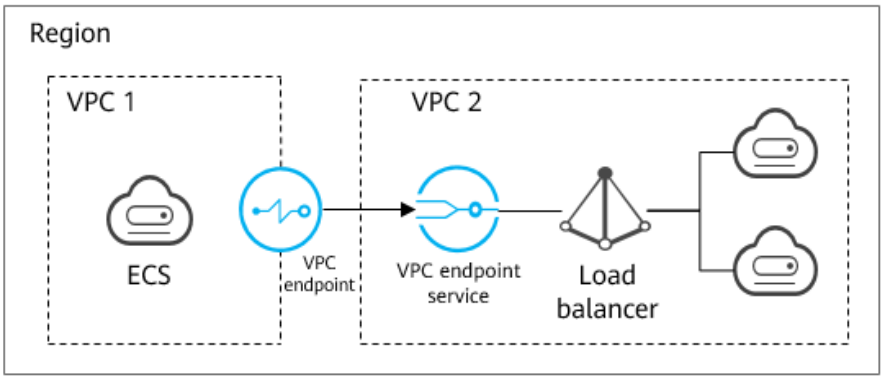
With VPCEP, you can access resources across VPCs in the same region.

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

The two VPCs can belong to the same or different accounts. This section uses the communications across two VPCs of the same account as an example.

For example, VPC 1 and VPC 2 belong to the same account. Configure a load balancer in VPC 2 as a VPC endpoint service and buy a VPC endpoint for VPC 1 so that the ECS in VPC 1 can access the load balancer in VPC 2 using a private IP address.

Figure 3-1 Cross-VPC communications



 Copyright © Huawei Technologies Co., Ltd.

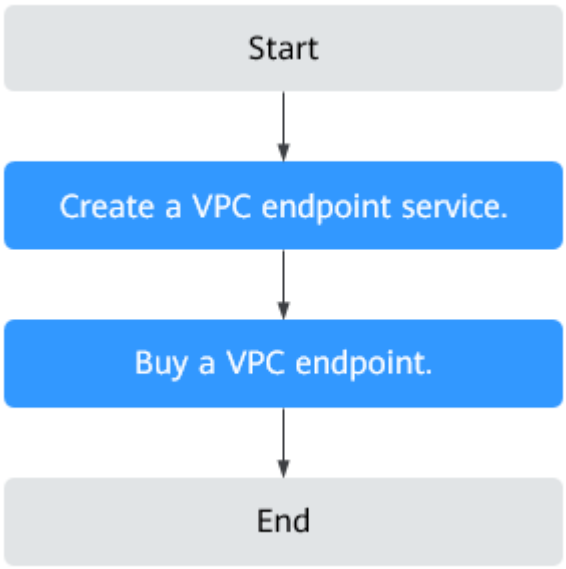
NOTE

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

Configuration Process

Figure 3-2 shows how to enable communications between two VPCs of the same account using VPCEP.

Figure 3-2 Cross-VPC communications



3.2 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 an elastic load balancer as an example backend service to describe how to create a VPC endpoint service.

Prerequisites

There are available backend resources in the same VPC.

Procedure

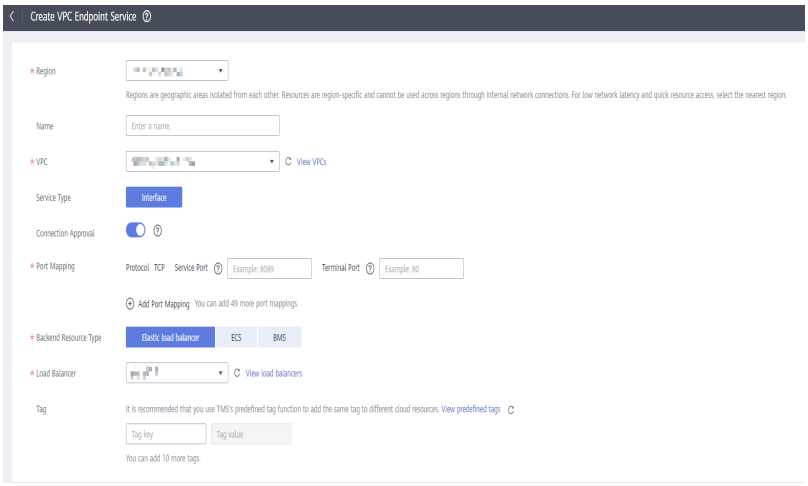
1. Log in to the management console.
2. Click in the upper left corner and select the required region and project.

 Copyright © Huawei Technologies Co., Ltd.

3. Choose **Service List** > **Networking** > **VPC Endpoint**.
4. In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoint Services** and click **Create VPC Endpoint Service**.

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

Figure 3-3 Create VPC Endpoint Service



5. Configure the required parameters.

Table 3-1 Required parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint service is deployed. Resources in different regions cannot communicate with each other over internal networks. Select the nearest region for lower network latency and faster access to resources.
Name	This parameter is optional. Specifies the name of the VPC endpoint service. The name can contain a maximum of 16 characters, including letters, digits, underscores (_), and hyphens (-). • If you do not enter a name, the system automatically generates a name in the *region.service_id* format. • If you enter a name, the system automatically generates a name in the *region.Name.service_id* format.
VPC	Specifies the VPC where the VPC endpoint service is deployed.
Service Type	Specifies the type of the VPC endpoint service. The type can only be **Interface**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
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 determine whether to enable or disable the connection approval. If connection approval is enabled, any VPC endpoint for connecting to the VPC endpoint service needs to be approved. For details, see step 7.
Port Mapping	Specifies the protocol and ports used for communications between the VPC endpoint service and VPC endpoint. The protocol is TCP. • **Service Port**: A service port is provided by the backend service bound to the endpoint service. • **Terminal Port**: A terminal port is provided by the VPC endpoint, allowing you to access the VPC endpoint service. The service and terminal port numbers range from **1** to **65535**. A maximum of 50 port mappings can be added at a time. **NOTE** Accessing a VPC endpoint service from a VPC endpoint is to access the service port from the associated terminal port.
Backend Resource Type	Specifies the type of the backend resource that provides services to be accessed. The following backend resources are supported: • **Elastic load balancer**: Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance. • **ECS**: Backend resources of this type serve as servers. • **BMS**: Backend resources of this type serve as servers. Example: **Elastic load balancer** **NOTE** For the security group associated with the backend resource configured for the VPC endpoint service, add an inbound rule, with the source IP address set to 198.19.0.0/16. For details, see **Adding a Security Group Rule** in the *Virtual Private Cloud User Guide*.
Load Balancer	When **Backend Resource Type** is set to **Elastic load balancer**, select the load balancer that provides services from the drop-down list. **NOTE** If an elastic load balancer is used as the backend resource, the source IP address received by the VPC endpoint service is not the real address of the client.

 Copyright © Huawei Technologies Co., Ltd.

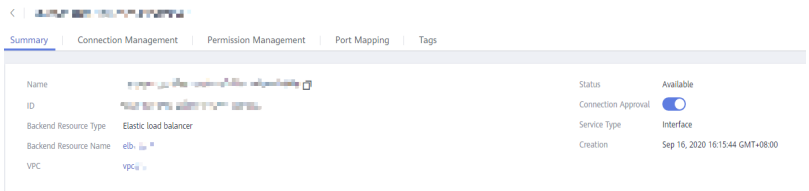
Parameter	Description
Tag	This parameter is optional. Specifies the VPC endpoint service tag, which consists of a key and a value. You can add a maximum of 10 tags to each VPC endpoint service. Tag keys and values must meet requirements listed in **Table 3-2**. **NOTE** If a predefined tag has been created on TMS, you can directly select the corresponding tag key and value. For details about predefined tags, see **Predefined Tag Overview**.

Table 3-2 Tag requirements for VPC endpoint services

Parameter	Requirement
Tag key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 36 Unicode characters. • Cannot start or end with a space or contain special characters =*<>\,|/
Tag value	• Cannot be left blank. • Can contain a maximum of 43 Unicode characters. • Cannot start or end with a space or contain special characters =*<>\,|/

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

Figure 3-4 Summary of the VPC endpoint service



 Copyright © Huawei Technologies Co., Ltd.

3.3 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 for connecting to the VPC endpoint service.

NOTE

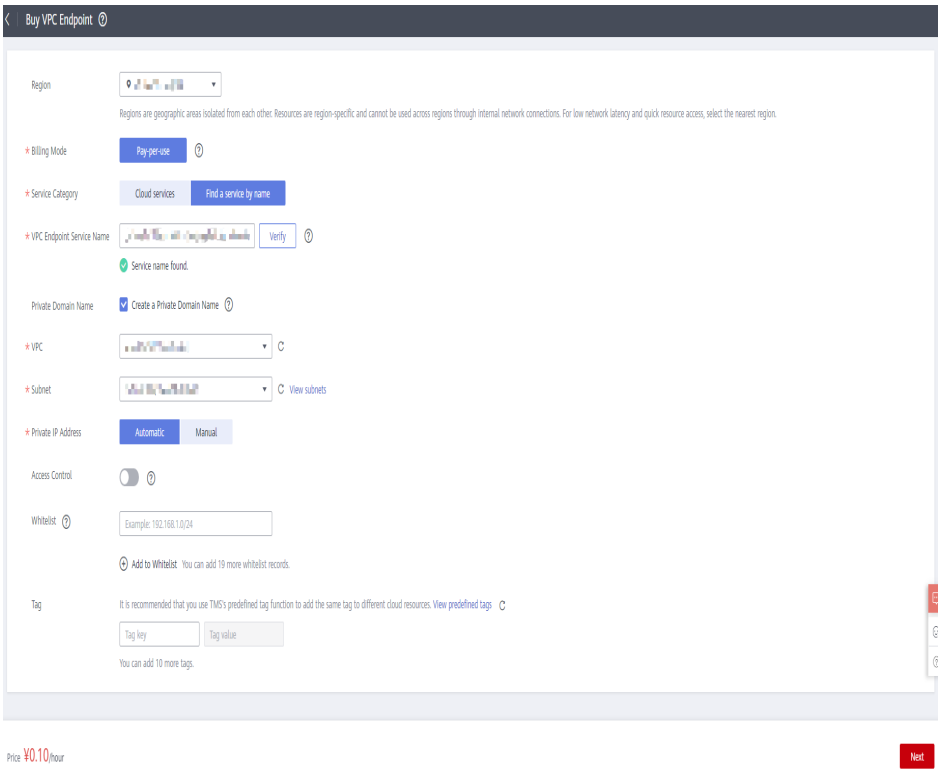
Select the same region and project as those of the VPC endpoint service.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the required region and project.
3. Choose **Service List** > **Networking** > **VPC Endpoint**.
4. On the **VPC Endpoints** page, click **Buy VPC Endpoint**.

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

   Figure 3-5 Buy VPC Endpoint (**Service Category** set to **Find a service by name**)

5. Set the required parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-3 Required parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint is located. This region is the same as that of the VPC endpoint service.
Billing Mode	Specifies the billing method of the VPC endpoint. VPC endpoints can be enabled or deleted at any time. VPC endpoints support only pay-per-use billing.
Service Category	There are two options: **Cloud services** or **Find a service by name**. • **Cloud services**: The target VPC endpoint service is a cloud service. • **Find a service by name**: The target VPC endpoint service is a private service of your own. Example: **Find a service by name**
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 step **8** and click **Verify**. • If **Service name found** is displayed, proceed with subsequent operations. • If **Service name not found** is displayed, check whether the region is the same as that of the connected VPC endpoint service or whether the entered service name is correct.
Private Domain Name	If you want to access a VPC endpoint using a domain name, select **Create a Private Domain Name** when creating a VPC endpoint. After the VPC endpoint is created, you can access it using the domain name. • For the gateway type, this parameter is unavailable. • For the interface type, this parameter is optional.
VPC	Specifies the VPC where the VPC endpoint is deployed.
Subnet	Specifies the subnet where the VPC endpoint is located.
Private IP Address	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. Specifies the private IP address of the VPC endpoint. You can select **Automatic** or **Manual**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Access Control	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. It controls IP addresses allowed to access the VPC endpoint. ● If access control is enabled, only IP addresses in the whitelist are allowed to access the VPC endpoint. ● If access control is disabled, all IP addresses are allowed to access the VPC endpoint.
Whitelist	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. Lists the IP addresses or CIDR blocks that are allowed to access the VPC endpoint. You can add a maximum of 20 records.
Tag	This parameter is optional. Specifies the VPC endpoint tag, which consists of a key and a value. You can add a maximum of 10 tags to each VPC endpoint. Tag keys and values must meet requirements listed in **Table 3-4**. **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**.

Table 3-4 Tag requirements for VPC endpoints

Parameter	Requirement
Tag key	● Cannot be left blank. ● Must be unique for each resource. ● Can contain a maximum of 36 Unicode characters. ● Cannot start or end with a space or contain special characters =*<>\,|/
Tag value	● Cannot be left blank. ● Can contain a maximum of 43 Unicode characters. ● Cannot start or end with a space or contain special characters =*<>\,|/

6. Confirm the specifications and click **Next**.

 Copyright © Huawei Technologies Co., Ltd.

- If all of the specifications are correct, click **Submit**.
- If any of the specifications are incorrect, click **Previous** to return to the previous page and modify the parameters as needed, and click **Submit**.

7. Manage the connection of the VPC endpoint.

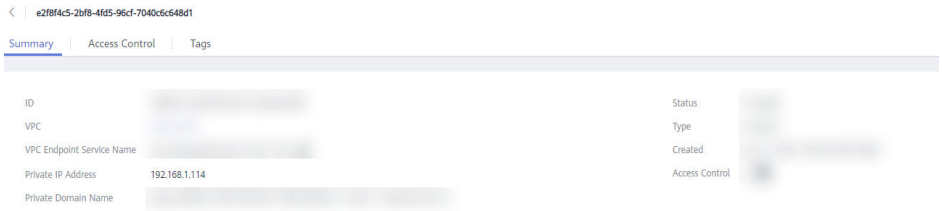
   If the status of the VPC endpoint changes to **Accepted**, the VPC endpoint is connected to the required VPC endpoint service. If the status is **Pending acceptance**, connection approval is enabled for the endpoint service, ask the owner of the endpoint service to perform the following operations:

   a. In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoint Services**.
   b. In the VPC endpoint service list, locate the target VPC endpoint service and click its name.
   c. On the displayed page, select the **Connection Management** tab.
      - If you allow a VPC endpoint to connect to this VPC endpoint service, locate the target VPC endpoint and click **Accept** in the **Operation** column.
      - If you refuse a VPC endpoint from connecting to this VPC endpoint service, click **Reject** in the **Operation** column.
   d. 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.

8. 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**.

   Figure 3-6 Summary of the VPC endpoint (for accessing an interface VPC endpoint service)

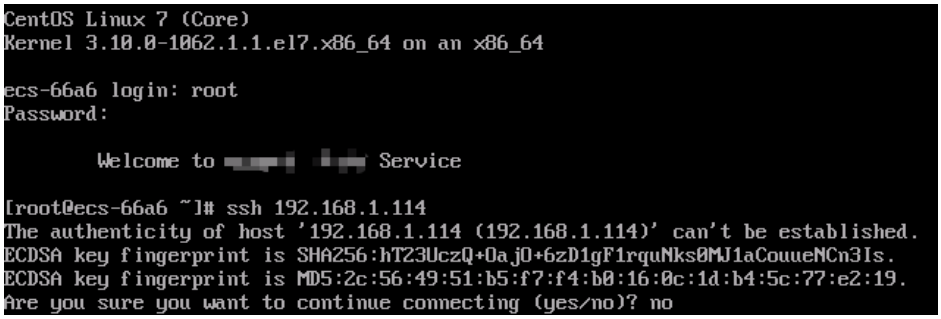
   You can use the private IP address or private domain name to access the VPC endpoint service.

Configuration Verification

Log in to an ECS in VPC 1 remotely and access the VPC endpoint using its private IP address or private domain name.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-7 Logging in to the ECS to access the VPC endpoint



 Copyright © Huawei Technologies Co., Ltd.

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

4.1 Overview

Scenarios

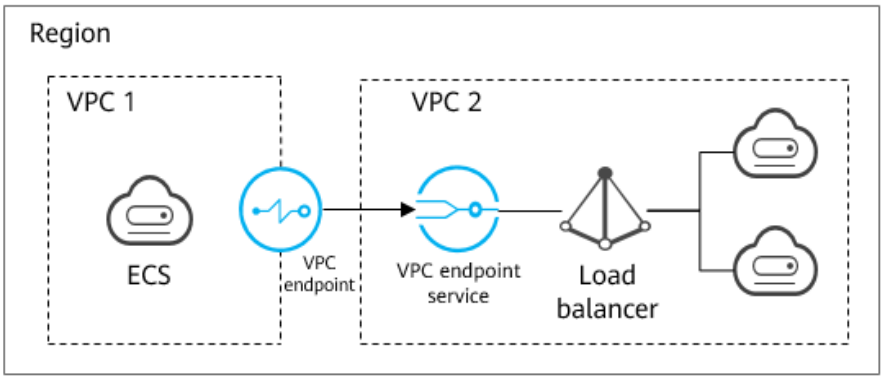
With VPCEP, you can access resources across VPCs in the same region.

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

The two VPCs can belong to the same or different accounts. This section focuses on the communications across two VPCs of different accounts.

For example, VPC 1 and VPC 2 belong to different accounts A and B, respectively. Configure a load balancer in VPC 2 as a VPC endpoint service and buy a VPC endpoint for VPC 1 so that the ECS in VPC 1 can access the load balancer in VPC 2 using a private IP address.

Figure 4-1 Cross-VPC communications



 Copyright © Huawei Technologies Co., Ltd.

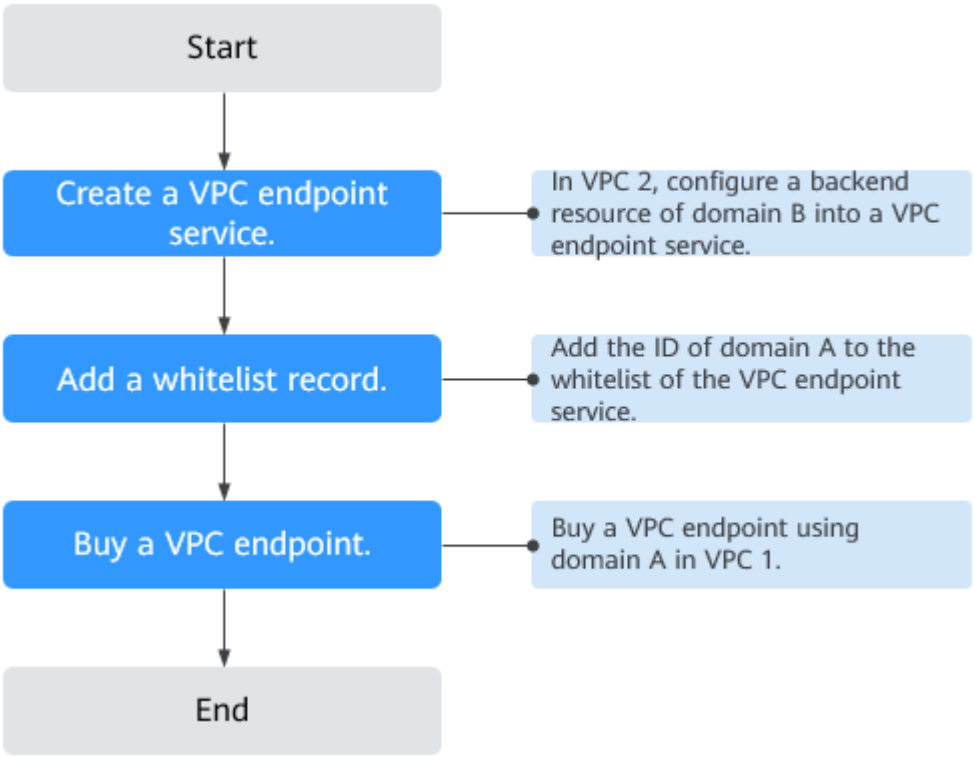
NOTE

- Only one-way communications from the VPC endpoint to the VPC endpoint service is 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**.

Cross-VPC Communications

Figure 4-2 shows how to enable communications between two VPCs of different accounts using VPCEP.

Figure 4-2 Cross-VPC communications flowchart



4.2 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 are available backend resources in the same VPC.

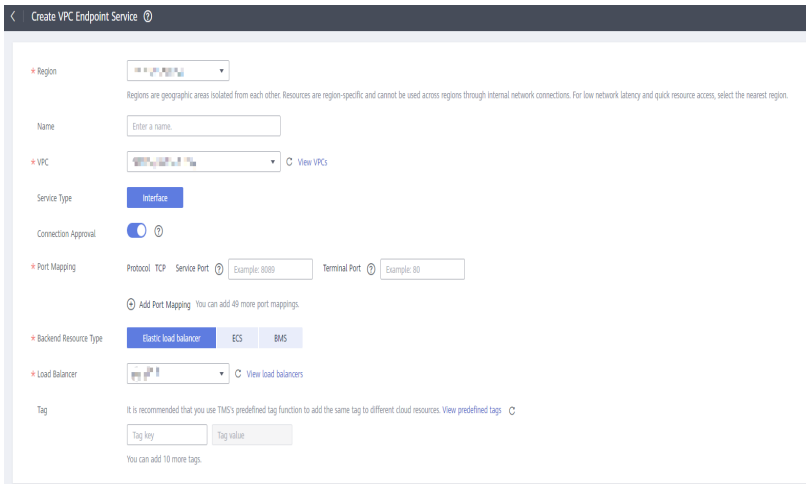
 Copyright © Huawei Technologies Co., Ltd.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the required region and project.
3. Choose **Service List** > **Networking** > **VPC Endpoint**.
4. In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoint Services** and click **Create VPC Endpoint Service**.

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

Figure 4-3 Create VPC Endpoint Service



5. Configure the required parameters.

Table 4-1 Required parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint service is deployed. Resources in different regions cannot communicate with each other over internal networks. Select the nearest region for lower network latency and faster access to resources.
Name	This parameter is optional. Specifies the name of the VPC endpoint service. The name can contain a maximum of 16 characters, including letters, digits, underscores (_), and hyphens (-). • If you do not enter a name, the system automatically generates a name in the *region.service_id* format. • If you enter a name, the system automatically generates a name in the *region.Name.service_id* format.
VPC	Specifies the VPC where the VPC endpoint service is deployed.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Service Type	Specifies the type of the VPC endpoint service. The type can only be **Interface**.
Connection Approval	Specifies whether the connection between a VPC endpoint and a VPC endpoint service requires approval from the owner of the VPC endpoint service. You can determine whether to enable or disable the connection approval. If connection approval is enabled, any VPC endpoint for connecting to the VPC endpoint service needs to be approved. For details, see step 7.
Port Mapping	Specifies the protocol and ports used for communications between the VPC endpoint service and VPC endpoint. The protocol is TCP. • **Service Port**: A service port is provided by the backend service bound to the endpoint service. • **Terminal Port**: A terminal port is provided by the VPC endpoint, allowing you to access the VPC endpoint service. The service and terminal port numbers range from **1** to **65535**. A maximum of 50 port mappings can be added at a time. **NOTE** Accessing a VPC endpoint service from a VPC endpoint is to access the service port from the associated terminal port.
Backend Resource Type	Specifies the type of the backend resource that provides services to be accessed. The following backend resources are supported: • **Elastic load balancer**: Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance. • **ECS**: Backend resources of this type serve as servers. • **BMS**: Backend resources of this type serve as servers. Example: **Elastic load balancer** **NOTE** For the security group associated with the backend resource configured for the VPC endpoint service, add an inbound rule, with the source IP address set to 198.19.0.0/16. For details, see **Adding a Security Group Rule** in the *Virtual Private Cloud User Guide*.
Load Balancer	When **Backend Resource Type** is set to **Elastic load balancer**, select the load balancer that provides services from the drop-down list. **NOTE** If an elastic load balancer is used as the backend resource, the source IP address received by the VPC endpoint service is not the real address of the client.

Copyright © Huawei Technologies Co., Ltd.

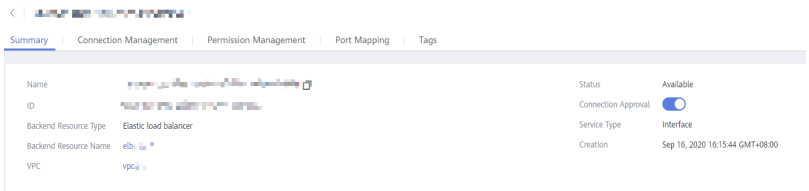
Parameter	Description
Tag	This parameter is optional. Specifies the VPC endpoint service tag, which consists of a key and a value. You can add a maximum of 10 tags to each VPC endpoint service. Tag keys and values must meet requirements listed in **Table 4-2**. **NOTE** If a predefined tag has been created on TMS, you can directly select the corresponding tag key and value. For details about predefined tags, see **Predefined Tag Overview**.

Table 4-2 Tag requirements for VPC endpoint services

Parameter	Requirement
Tag key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 36 Unicode characters. • Cannot start or end with a space or contain special characters =*<>\,|/
Tag value	• Cannot be left blank. • Can contain a maximum of 43 Unicode characters. • Cannot start or end with a space or contain special characters =*<>\,|/

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

Figure 4-4 Summary of the VPC endpoint service



 Copyright © Huawei Technologies Co., Ltd.

4.3 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 an authorized account ID to or delete it from the whitelist of the endpoint service.

The following operations describe how to obtain your own account ID and add it to the whitelist of an existing VPC endpoint service in another account.

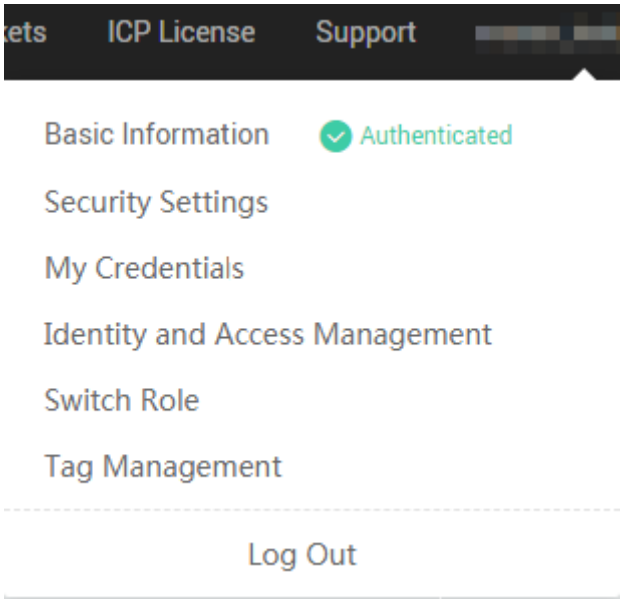
Prerequisites

The required VPC endpoint service already exists.

Obtain the ID of Your Own Account

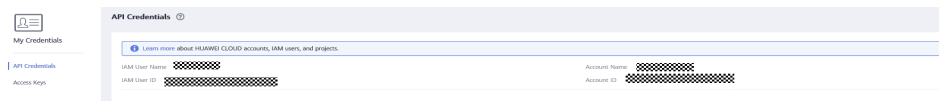
1. Log in to the management console.
2. Click **My Credentials** under the account.

Figure 4-5 My Credentials



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

Figure 4-6 Account ID

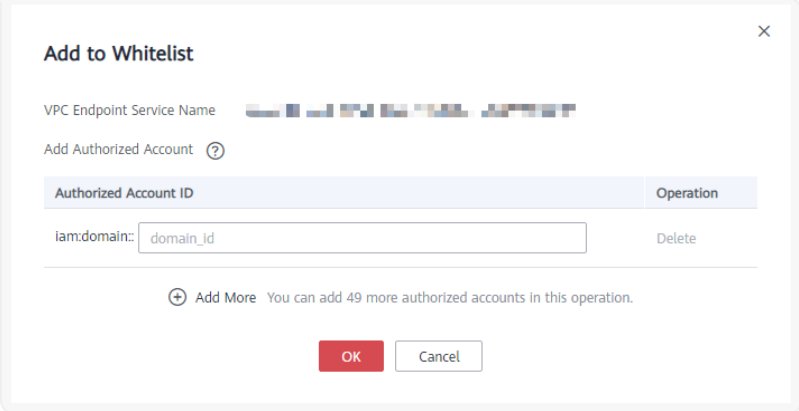


 Copyright © Huawei Technologies Co., Ltd.

Add an Authorized Account ID to the Whitelist of a VPC Endpoint Service

1. Log in to the management console.
2. Click in the upper left corner and select the required region and project.
3. Choose **Service List** > **Networking** > **VPC Endpoint**.
4. In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoint Services**.
5. In the VPC endpoint service list, locate the target VPC endpoint service and click its name.
6. On the displayed page, select the **Permission Management** tab and click **Add to Whitelist**.
7. Enter an authorized account ID in the required format and click **OK**.

Figure 4-7 Add to Whitelist



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.

8. Click **OK**.

4.4 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

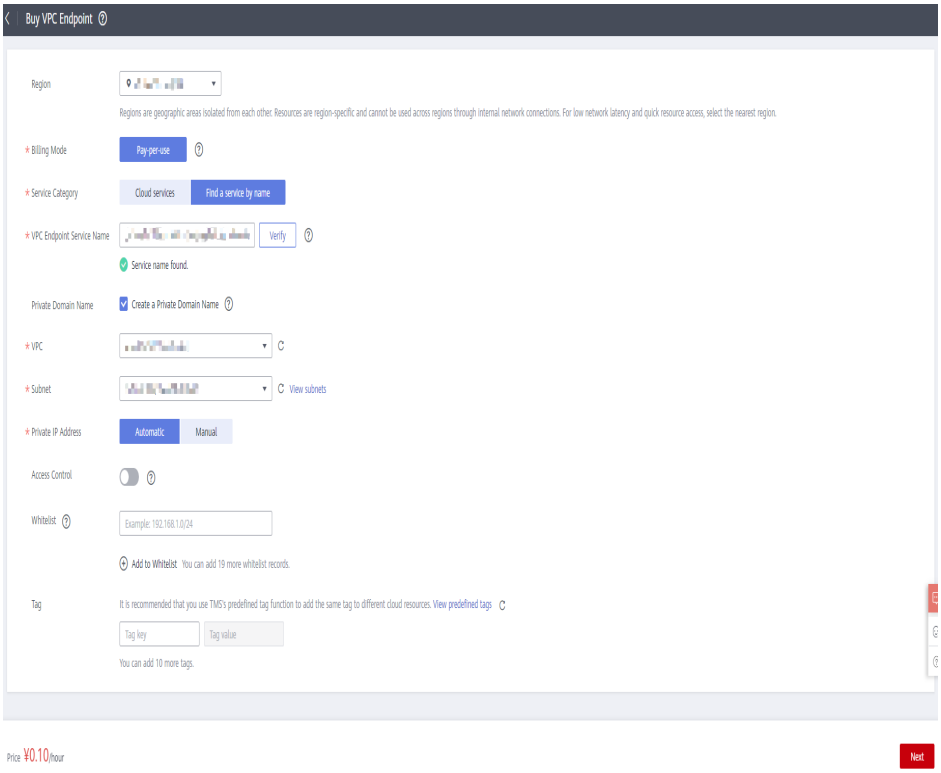
Select the same region and project as those of the VPC endpoint service.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the required region and project.
3. Choose **Service List** > **Networking** > **VPC Endpoint**.
4. On the **VPC Endpoints** page, click **Buy VPC Endpoint**.
   The **Buy VPC Endpoint** page is displayed.

   Figure 4-8 Buy VPC Endpoint (**Service Category** set to **Find a service by name**)

5. Set the required parameters.

   Table 4-3 Required parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint is located. This region is the same as that of the VPC endpoint service.
Billing Mode	Specifies the billing method of the VPC endpoint. VPC endpoints can be enabled or deleted at any time. VPC endpoints support only pay-per-use billing.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Service Category	There are two options: **Cloud services** or **Find a service by name**. • **Cloud services**: The target VPC endpoint service is a cloud service. • **Find a service by name**: The target VPC endpoint service is a private service of your own. Example: **Find a service by name**
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 step **8** and click **Verify**. • If **Service name found** is displayed, proceed with subsequent operations. • If **Service name not found** is displayed, check whether the region is the same as that of the connected VPC endpoint service or whether the entered service name is correct.
Private Domain Name	If you want to access a VPC endpoint using a domain name, select **Create a Private Domain Name** when creating a VPC endpoint. After the VPC endpoint is created, you can access it using the domain name. • For the gateway type, this parameter is unavailable. • For the interface type, this parameter is optional.
VPC	Specifies the VPC where the VPC endpoint is deployed.
Subnet	Specifies the subnet where the VPC endpoint is located.
Private IP Address	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. Specifies the private IP address of the VPC endpoint. You can select **Automatic** or **Manual**.
Access Control	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. It controls IP addresses allowed to access the VPC endpoint. • If access control is enabled, only IP addresses in the whitelist are allowed to access the VPC endpoint. • If access control is disabled, all IP addresses are allowed to access the VPC endpoint.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Whitelist	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. Lists the IP addresses or CIDR blocks that are allowed to access the VPC endpoint. You can add a maximum of 20 records.
Tag	This parameter is optional. Specifies the VPC endpoint tag, which consists of a key and a value. You can add a maximum of 10 tags to each VPC endpoint. Tag keys and values must meet requirements listed in **Table 4-4**. **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**.

Table 4-4 Tag requirements for VPC endpoints

Parameter	Requirement
Tag key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 36 Unicode characters. • Cannot start or end with a space or contain special characters =*<>\,|/
Tag value	• Cannot be left blank. • Can contain a maximum of 43 Unicode characters. • Cannot start or end with a space or contain special characters =*<>\,|/

6. Confirm the specifications and click **Next**.
   - If all of the specifications are correct, click **Submit**.
   - If any of the specifications are incorrect, click **Previous** to return to the previous page and modify the parameters as needed, and click **Submit**.
7. 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 endpoint service, ask the owner of the endpoint service to perform the following operations:

 Copyright © Huawei Technologies Co., Ltd.

a. In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoint Services**.

b. In the VPC endpoint service list, locate the target VPC endpoint service and click its name.

c. On the displayed page, select the **Connection Management** tab.

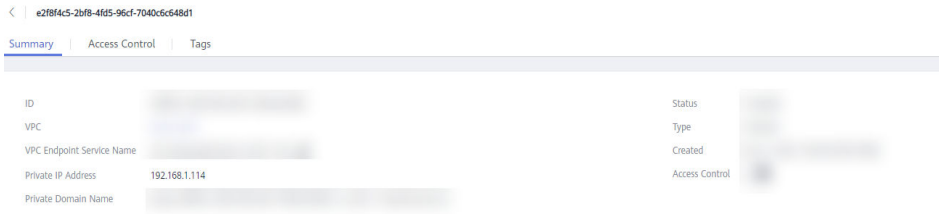
   - If you allow a VPC endpoint to connect to this VPC endpoint service, locate the target VPC endpoint and click **Accept** in the **Operation** column.
   - If you refuse a VPC endpoint from connecting to this VPC endpoint service, click **Reject** in the **Operation** column.

d. 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.

8. 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**.

   Figure 4-9 Summary of the VPC endpoint (for accessing an interface VPC endpoint service)

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

 Copyright © Huawei Technologies Co., Ltd.

5 Configuring a VPC Endpoint for Accessing OBS Using the OBS Private Address

5.1 Overview

Scenarios

If you want to access a cloud service like OBS from an IDC, you can connect the IDC to your VPC using a VPN connection or a direct connection and then connect your VPC to a cloud service using a VPC endpoint.

This section describes how to configure a VPC endpoint to access OBS using its private address from an IDC.

NOTE

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

Figure 5-1 Accessing OBS using its private address from an IDC

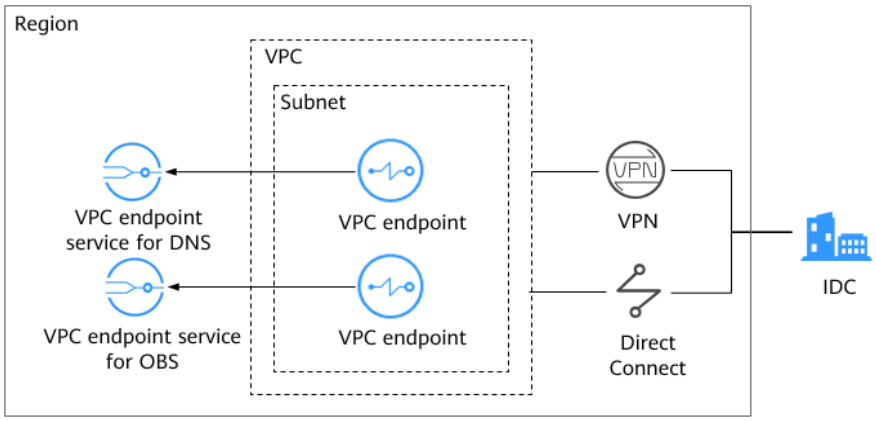


Figure 5-1 shows the process of connecting an IDC to a VPC over VPN or Direct Connect to access DNS and OBS using two VPC endpoints, respectively.

 Copyright © Huawei Technologies Co., Ltd.

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.

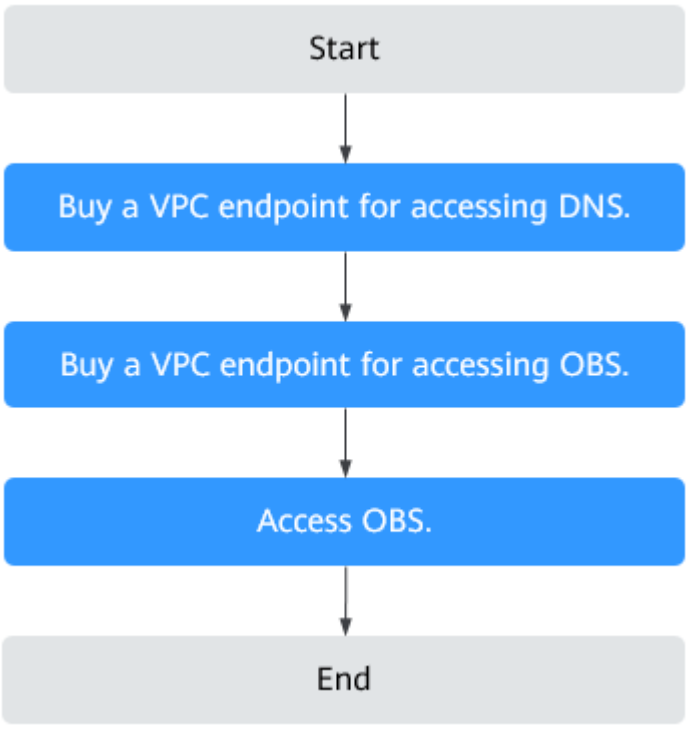
The following VPC endpoint services are required:

- VPC endpoint service for DNS: resolves the OBS domain name at the IDC.
  LA-Mexico City1: **com.myhuaweicloud.na-mexico-1.dns**
- VPC endpoint service for OBS: provides the OBS service for the IDC.
  LA-Mexico City1: **com.myhuaweicloud.na-mexico-1.obs**

Configuration Process

Figure 5-2 shows the process for configuring a VPC endpoint to access OBS using its private address from an IDC.

Figure 5-2 Configuration flowchart



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

Scenarios

This section describes how to buy a VPC endpoint for accessing a DNS server, in order to forward requests of resolving OBS domain names.

Prerequisites

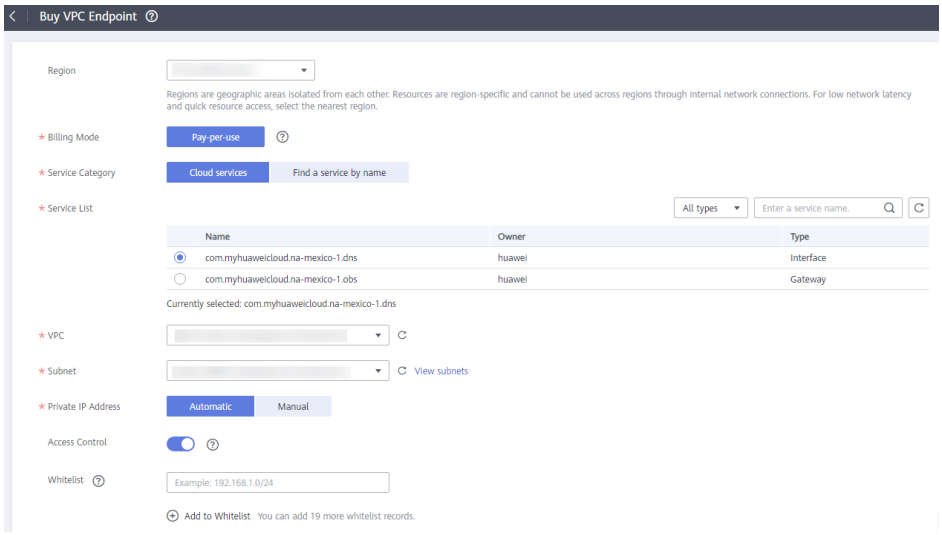
The required VPC endpoint service already exists.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the required region and project.
3. Choose **Service List** > **Networking** > **VPC Endpoint**.
4. On the **VPC Endpoints** page, click **Buy VPC Endpoint**.
   The **Buy VPC Endpoint** page is displayed.

   Figure 5-3 Buy VPC Endpoint (**Service Category** set to **Cloud service**)

5. Set the required parameters.

   Table 5-1 Required parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint is located. Resources in different regions cannot communicate with each other over internal networks. Select the nearest region for lower network latency and faster access to resources.
Billing Mode	Specifies the billing method of the VPC endpoint. VPC endpoints can be enabled or deleted at any time. VPC endpoints support only pay-per-use billing.
Service Category	There are two options: **Cloud services** or **Find a service by name**. • **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. Example: **Cloud services**

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Service List	This parameter is available only when you select **Cloud services** for **Service Category**. The VPC endpoint service has been created by operations people and you can use it without having to perform the creation operation. Example: **com.myhuaweicloud.na-mexico-1.dns**
Private Domain Name	If you want to access a VPC endpoint using a domain name, select **Create a Private Domain Name** when creating a VPC endpoint. After the VPC endpoint is created, you can access it using the domain name. This parameter can only be configured for VPC endpoints of the interface type, and its setting depends on the type of target VPC endpoint services: ● For the gateway type, this parameter is unavailable. ● For the interface type, this parameter is optional.
VPC	Specifies the VPC where the VPC endpoint is 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 located.
Private IP Address	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. Specifies the private IP address of the VPC endpoint. You can select **Automatic** or **Manual**.
Access Control	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. It controls IP addresses allowed to access the VPC endpoint. ● If access control is enabled, only IP addresses in the whitelist are allowed to access the VPC endpoint. ● If access control is disabled, all IP addresses are allowed to access the VPC endpoint.
Whitelist	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. Lists the IP addresses or CIDR blocks that are allowed to access the VPC endpoint. You can add a maximum of 20 records.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Tag	This parameter is optional. Specifies the VPC endpoint tag, which consists of a key and a value. You can add a maximum of 10 tags to each VPC endpoint. Tag keys and values must meet requirements listed in **Table 5-2**. **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**.

Table 5-2 Tag requirements for VPC endpoints

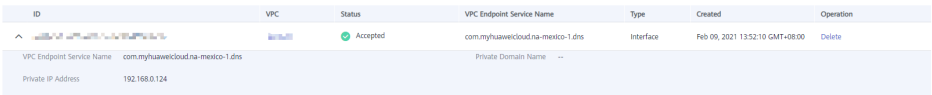
Parameter	Requirement
Tag key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 36 Unicode characters. • Cannot start or end with a space or contain special characters =*<>\,|/
Tag value	• Cannot be left blank. • Can contain a maximum of 43 Unicode characters. • Cannot start or end with a space or contain special characters =*<>\,|/

6. Confirm the specifications and click **Next**.
   - If all of the specifications are correct, click **Submit**.
   - If any of the specifications are incorrect, click **Previous** to return to the previous page and modify the parameters as needed, and click **Submit**.
7. 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.
8. In the VPC endpoint list, click the ID of the target VPC endpoint to view its details.

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

Figure 5-4 Summary of the VPC endpoint



 Copyright © Huawei Technologies Co., Ltd.

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

Scenarios

This section describes how to buy a VPC endpoint to access OBS from an IDC.

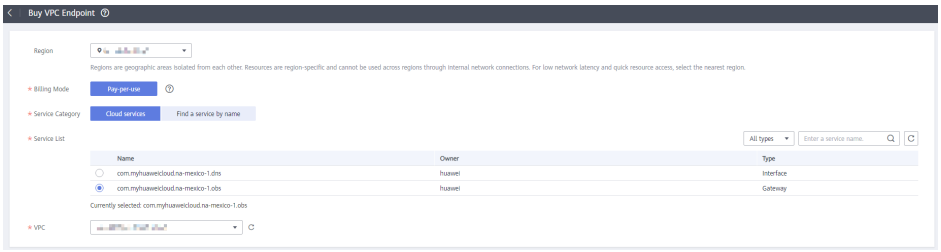
Prerequisites

The required VPC endpoint service already exists.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the required region and project.
3. Choose **Service List** > **Networking** > **VPC Endpoint**.
4. On the **VPC Endpoints** page, click **Buy VPC Endpoint**.
   The **Buy VPC Endpoint** page is displayed.

   Figure 5-5 Buy VPC Endpoint (**Service Category** set to **Cloud service**)

5. Set the required parameters.

   Table 5-3 Required parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint is located. Resources in different regions cannot communicate with each other over internal networks. Select the nearest region for lower network latency and faster access to resources.
Billing Mode	Specifies the billing method of the VPC endpoint. VPC endpoints can be enabled or deleted at any time. VPC endpoints support only pay-per-use billing.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Service Category	There are two options: **Cloud services** or **Find a service by name**. • **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. Example: **Cloud services**
Service List	This parameter is available only when you select **Cloud services** for **Service Category**. The VPC endpoint service has been created by operations people and you can use it without having to perform the creation operation. Example: **com.myhuaweicloud.na-mexico-1.obs**
VPC	Specifies the VPC where the VPC endpoint is deployed.
Route Table	This parameter is available only when you create a VPC endpoint for connecting to a gateway VPC endpoint service. **NOTE** This parameter is available only in the regions where the route table function is enabled. Select a route table required for the VPC where the VPC endpoint is located. For details about how to add a route, see **Adding a Custom Route** in the *Virtual Private Cloud User Guide*.
Tag	This parameter is optional. Specifies the VPC endpoint tag, which consists of a key and a value. You can add a maximum of 10 tags to each VPC endpoint. Tag keys and values must meet requirements listed in **Table 5-4**. **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**.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-4 Tag requirements for VPC endpoints

Parameter	Requirement
Tag key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 36 Unicode characters. • Cannot start or end with a space or contain special characters =*<>\,|/
Tag value	• Cannot be left blank. • Can contain a maximum of 43 Unicode characters. • Cannot start or end with a space or contain special characters =*<>\,|/

6. Confirm the specifications and click **Next**.
   - If all of the specifications are correct, click **Submit**.
   - If any of the specifications are incorrect, click **Previous** to return to the previous page and modify the parameters as needed, and click **Submit**.
7. 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.
8. In the VPC endpoint list, click the ID of the target VPC endpoint to view its details.

Figure 5-6 Summary of the VPC endpoint



5.4 Step 3: Access OBS

Scenarios

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

Prerequisites

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

- The local subnet of the VPC that interconnects with your VPN contains the OBS CIDR block 100.125.0.0/16.

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

 Copyright © Huawei Technologies Co., Ltd.

- The CIDR block of the virtual gateway associated with your direct connection contains the OBS CIDR block 100.125.0.0/16.

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

Procedure

1. In the VPC endpoint list, locate the target VPC endpoint and click the ID of the endpoint to view its details.
2. Add DNS records on the DNS server at your local 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 operating systems. For details, see the DNS software operation documents.

   This step uses the common DNS software Bind as an example to configure forwarding rules in the UNIX operating system as follows:

   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.

   Take the OBS endpoint in region LA-Mexico City1 as an example:

   zone "com.myhuaweicloud.na-mexico-1.obs" {

   type forward;

   forward only;

   forwarders{ *xx.xx.xx.xx*;**};**

   };

   NOTE

   - If no DNS server is available at your local data center, add the private IP address of the VPC endpoint in file **/etc/resolv.conf**.
   - *xx.xx.xx.xx* is the private IP address obtained in step 1.
3. Configure a DNS route from your local data center to the VPN gateway or Direct Connect gateway.

   xx.xx.xx.xx indicates the private IP address of the VPC endpoint. To access DNS using a VPN connection or a direct connection, ensure that traffic from your local data center to DNS is directed to the VPN gateway or Direct Connect gateway.

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

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

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- *xx.xx.xx.xx* is the private IP address obtained in step 1.
- *xxx.xxx.xxx.xxx* indicates the IP address of the Direct Connect or VPN gateway created at your local data center.

4. Configure an OBS route from the local data center to the VPN or Direct Connect gateway.

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

   Configure a permanent route at your local data center and specify the Direct Connect or VPN gateway as the next hop for accessing OBS.

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

   NOTE

   xxx.xxx.xxx.xxx indicates the IP address of the Direct Connect or VPN gateway created at your local data center.

5. At the local data center, run the following command to verify the connectivity with OBS:

   telnet *bucket.endpoint*

   In the command:

   – **bucket**: indicates the bucket name.

   – **endpoint**: indicates the endpoint information about OBS.

   Example: **telnet** *bucket*.**obs.na-mexico-1.myhuaweicloud.com**

   NOTE

   Obtain OBS endpoint information at **Regions and Endpoints**.

 Copyright © Huawei Technologies Co., Ltd.

6 Change History

Released On	Description
2020-11-13	This issue is the fourth official release. Added: • **Operation Guide** • **Preparations**
2019-07-10	This issue is the third official release. Updated all screenshots in this document.
2019-04-15	This issue is the second official release. Described the usage of VPCEP in two scenarios.
2018-11-30	This issue is the first official release.

 Copyright © Huawei Technologies Co., Ltd.