VPC Endpoint

Getting Started

Issue 01

Date 2023-08-18

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2023. 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

HUAWEI 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

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 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: ● **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 on-premises data center. For details, see the following sections: **Configuring a VPC Endpoint for Accessing the Private IP Address of OBS over Private Networks**

Copyright © Huawei Technologies Co., Ltd.

2 Preparations

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

- Registering with Huawei Cloud

Registering with Huawei Cloud

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 application. You can only use it on the Huawei Cloud management console.

1. Visit **https://www.huaweicloud.com/eu/**.
2. Click **Register**.

   The registration page is displayed. Enter the required information. After your registration is successful, the system automatically redirects you to your personal information page.

Then your account will have permissions to access the VPCEP service and all other Huawei Cloud services.

Copyright © Huawei Technologies Co., Ltd.

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

3.1 Overview

Scenarios

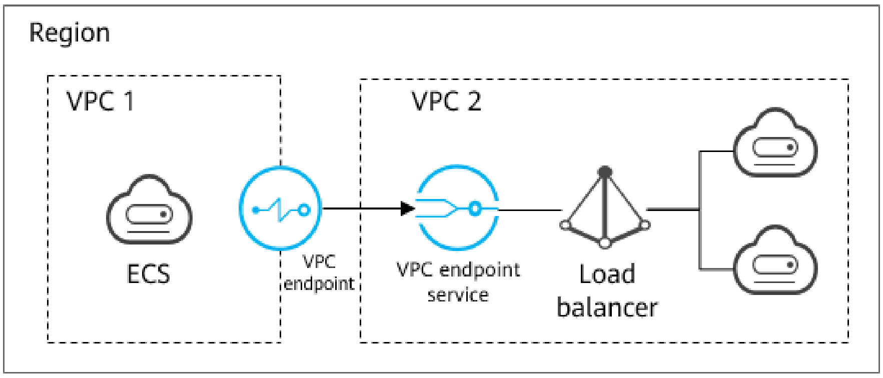
With VPCEP, you can access resources across VPCs in the same region.

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.

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

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.

Figure 3-1 Cross-VPC communications



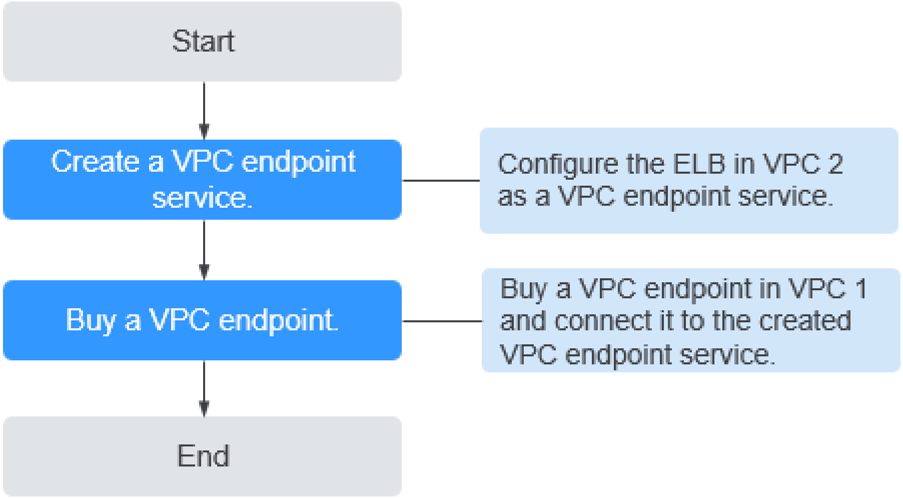
NOTE

- 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**.

Configuration Process

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

Figure 3-2 Cross-VPC communications


Start
Create a VPC endpoint service.
Configure the ELB in VPC 2 as a VPC endpoint service.
Buy a VPC endpoint.
Buy a VPC endpoint in VPC 1 and connect it to the created VPC endpoint service.
End

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 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.
3. Click **Service List** and choose **Networking** > **VPC Endpoint**.

4. In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoint Services**. In the upper right corner, click **Create VPC Endpoint Service**.

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

5. Configure required parameters.

Table 3-1 Parameters for creating a VPC endpoint service

Parameter	Description
Region	Specifies the region where the VPC endpoint service is to be deployed. Resources in different regions cannot communicate with each other over an intranet. For lower latency and quicker access, select the nearest region.
Name	This parameter is optional. Specifies the name of the VPC endpoint service. The name can contain a maximum of 16 characters, including letters, digits, underscores (_), and hyphens (-). ● If you do not enter a name, the system generates a name in **{region}.{service_id}** format. ● If you enter a name, the system generates a name in **{region}.{Name}.{service_id}** format.
VPC	Specifies the VPC where the VPC endpoint service is to be deployed.
Service Type	Specifies the type of the VPC endpoint service. The type can only be **Interface**.
Connection Approval	Specifies whether the connection between a VPC endpoint and a VPC endpoint service requires approval from the owner of the VPC endpoint service. You can enable or disable **Connection Approval**. When **Connection Approval** is enabled, any VPC endpoint for connecting to the VPC endpoint service needs to be approved. For details, see step 7.

Parameter	Description
Port Mapping	Specifies the protocol and ports used for communications between the VPC endpoint service and a VPC endpoint. The protocol is TCP. ● **Service Port**: provided by the backend resource bound to the VPC endpoint service. ● **Terminal Port**: provided by the VPC endpoint, allowing you to access the VPC endpoint service. The service and terminal port numbers range from **1** to **65535**. A maximum of 50 port mappings can be added at a time. **NOTE** Accessing a VPC endpoint service from a VPC endpoint is to access the service port from the associated terminal port.
Backend Resource Type	Specifies the backend resource that provides services to be accessed. The following backend resource types are supported: ● **Elastic load balancer**: Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance. ● **ECS**: Backend resources of this type serve as servers. ● **BMS**: Backend resources of this type serve as servers. In this example, select **Elastic load balancer**. **NOTE** For the security group associated with the backend resource configured for the VPC endpoint service, add an inbound rule, with **Source** set to **198.19.128.0/17**. For details, see **Adding a Security Group Rule** in the *Virtual Private Cloud User Guide*.
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.
Tag	This parameter is optional. Specifies the VPC endpoint service tag, which consists of a key and a value. You can add up to 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

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

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 its details.

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.

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. Click **Service List** and choose **Networking** > **VPC Endpoint**.
4. On the **VPC Endpoints** page, click **Buy VPC Endpoint**.

   The **Buy VPC Endpoint** page is displayed.
5. Configure required parameters.

Table 3-3 VPC endpoint parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint is to be located. This region is the same as that of the VPC endpoint service.
Billing Mode	Specifies the billing mode of the VPC endpoint. VPC endpoints can be used or deleted at any time. VPC endpoints support only pay-per-use billing based on the usage duration.
Service Category	There are two options: ● **Cloud services**: Select this value if the target VPC endpoint service is a cloud service. ● **Find a service by name**: Select this value if the target VPC endpoint service is a private service of your own. In this example, select **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 name entered is correct.
Create a Private Domain Name	If you want to access a VPC endpoint using a domain name, select **Create a Private Domain Name** when buying a VPC endpoint. 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	Specifies the subnet where the VPC endpoint is to be 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 **Automatically assign** or **Manually specify**.

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 and CIDR blocks that are allowed to access the VPC endpoint. ● If **Access Control** is enabled, only IP addresses or CIDR blocks in the whitelist are allowed to access the VPC endpoint. ● If **Access Control** is disabled, any IP address or CIDR block can access the VPC endpoint.
Whitelist	This parameter is available 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 up to 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 characters. ● Cannot start or end with a space or contain special characters =*<>\,|/
Tag value	● Cannot be left blank. ● Can contain a maximum of 43 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 VPC endpoint service, ask the owner of the VPC endpoint service to perform the following operations:

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

   b. 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 do not allow a VPC endpoint to connect 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.

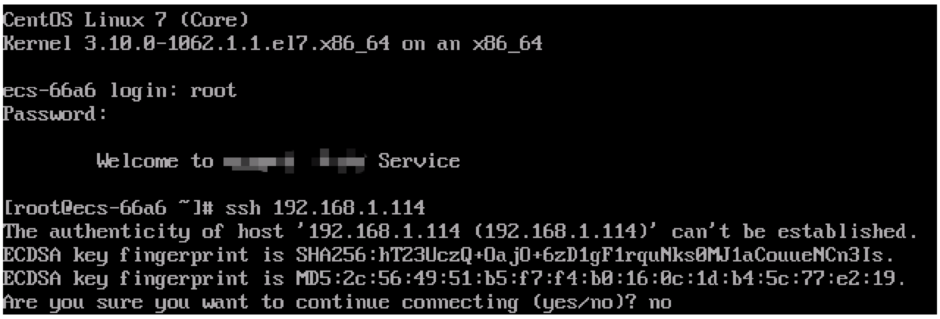
   After a VPC endpoint is created, a private IP address is assigned together with a private domain name if you select **Create a Private Domain Name** during creation.

   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 and access the private IP address or private domain name of the VPC endpoint.

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



```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.1.1.el7.x86_64 on an x86_64

ecs-66a6 login: root
Password:

        Welcome to [redacted] [redacted] Service

[root@ecs-66a6 ~]# ssh 192.168.1.114
The authenticity of host '192.168.1.114 (192.168.1.114)' can't be established.
ECDSA key fingerprint is SHA256:hT23UczQ+OajO+6zD1gF1rquNks0MJ1aCouueNCn3Is.
ECDSA key fingerprint is MD5:2c:56:49:51:b5:f7:f4:b0:16:0c:1d:b4:5c:77:e2:19.
Are you sure you want to continue connecting (yes/no)? no
```

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

4.1 Overview

Scenarios

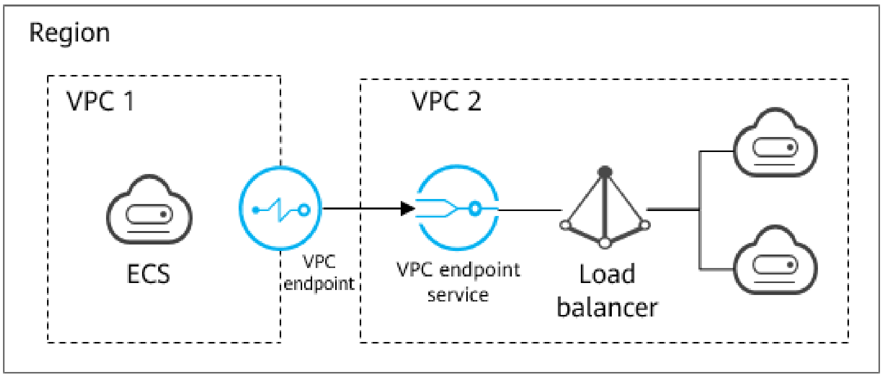
With VPCEP, you can access resources across VPCs in the same region.

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.

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

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 the private IP address.

Figure 4-1 Cross-VPC communications



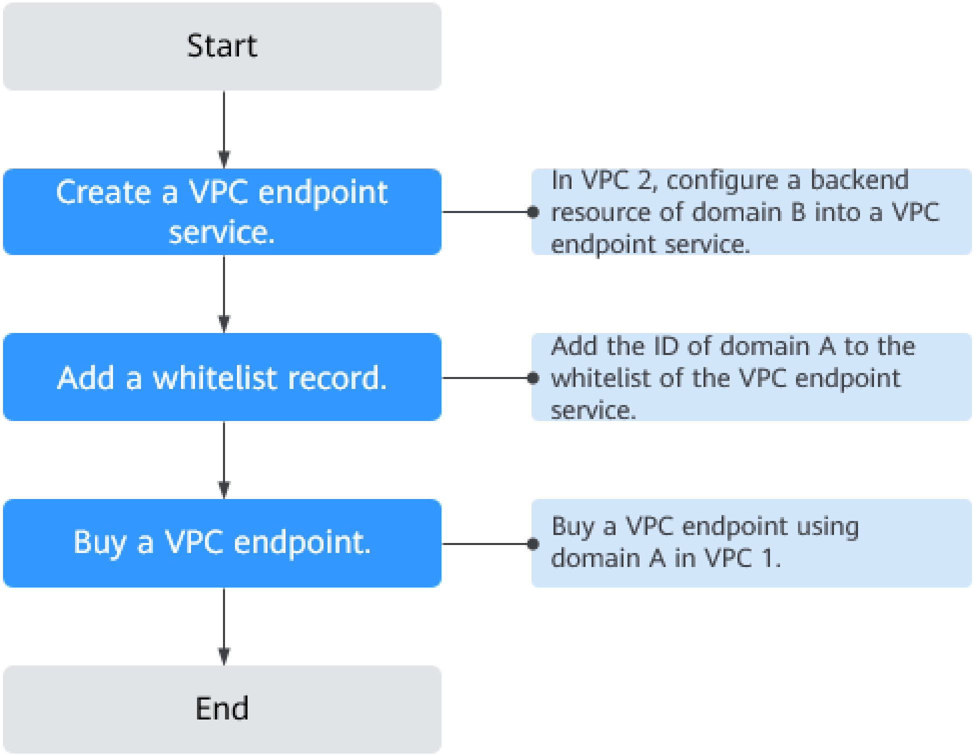
NOTE

- 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**.

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


Start
Create a VPC endpoint service.
In VPC 2, configure a backend resource of domain B into a VPC endpoint service.
Add a whitelist record.
Add the ID of domain A to the whitelist of the VPC endpoint service.
Buy a VPC endpoint.
Buy a VPC endpoint using domain A in VPC 1.
End

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.

Procedure

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

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

5. Configure required parameters.

Table 4-1 Parameters for creating a VPC endpoint service

Parameter	Description
Region	Specifies the region where the VPC endpoint service is to be deployed. Resources in different regions cannot communicate with each other over an intranet. For lower latency and quicker access, select the nearest region.
Name	This parameter is optional. Specifies the name of the VPC endpoint service. The name can contain a maximum of 16 characters, including letters, digits, underscores (_), and hyphens (-). ● If you do not enter a name, the system generates a name in **{region}.{service_id}** format. ● If you enter a name, the system generates a name in **{region}.{Name}.{service_id}** format.
VPC	Specifies the VPC where the VPC endpoint service is to be deployed.
Service Type	Specifies the type of the VPC endpoint service. The type can only be **Interface**.
Connection Approval	Specifies whether the connection between a VPC endpoint and a VPC endpoint service requires approval from the owner of the VPC endpoint service. You can enable or disable **Connection Approval**. When **Connection Approval** is enabled, any VPC endpoint for connecting to the VPC endpoint service needs to be approved. For details, see step 7.

Parameter	Description
Port Mapping	Specifies the protocol and ports used for communications between the VPC endpoint service and a VPC endpoint. The protocol is TCP. ● **Service Port**: provided by the backend resource bound to the VPC endpoint service. ● **Terminal Port**: provided by the VPC endpoint, allowing you to access the VPC endpoint service. The service and terminal port numbers range from **1** to **65535**. A maximum of 50 port mappings can be added at a time. **NOTE** Accessing a VPC endpoint service from a VPC endpoint is to access the service port from the associated terminal port.
Backend Resource Type	Specifies the backend resource that provides services to be accessed. The following backend resource types are supported: ● **Elastic load balancer**: Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance. ● **ECS**: Backend resources of this type serve as servers. ● **BMS**: Backend resources of this type serve as servers. In this example, select **Elastic load balancer**. **NOTE** For the security group associated with the backend resource configured for the VPC endpoint service, add an inbound rule, with **Source** set to **198.19.128.0/17**. For details, see **Adding a Security Group Rule** in the *Virtual Private Cloud User Guide*.
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.
Tag	This parameter is optional. Specifies the VPC endpoint service tag, which consists of a key and a value. You can add up to 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 characters. ● Cannot start or end with a space or contain special characters =*<>\,|/
Tag value	● Cannot be left blank. ● Can contain a maximum of 43 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 its details.

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 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.

Add AccountIDs to Be Authorized to the Whitelist of a VPC Endpoint Service

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

   NOTE

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

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.

Procedure

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

   The **Buy VPC Endpoint** page is displayed.
5. Configure required parameters.

Table 4-3 VPC endpoint parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint is to be located. This region is the same as that of the VPC endpoint service.

Parameter	Description
Billing Mode	Specifies the billing mode of the VPC endpoint. VPC endpoints can be used or deleted at any time. VPC endpoints support only pay-per-use billing based on the usage duration.
Service Category	There are two options: ● **Cloud services**: Select this value if the target VPC endpoint service is a cloud service. ● **Find a service by name**: Select this value if the target VPC endpoint service is a private service of your own. In this example, select **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 name entered is correct.
Create a Private Domain Name	If you want to access a VPC endpoint using a domain name, select **Create a Private Domain Name** when buying a VPC endpoint. 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	Specifies the subnet where the VPC endpoint is to be 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 **Automatically assign** or **Manually specify**.
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 and CIDR blocks that are allowed to access the VPC endpoint. ● If **Access Control** is enabled, only IP addresses or CIDR blocks in the whitelist are allowed to access the VPC endpoint. ● If **Access Control** is disabled, any IP address or CIDR block can access the VPC endpoint.

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 up to 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 characters. ● Cannot start or end with a space or contain special characters =*<>\,|/
Tag value	● Cannot be left blank. ● Can contain a maximum of 43 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 VPC endpoint service, ask the owner of the VPC endpoint service to perform the following operations:

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

   b. 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 do not allow a VPC endpoint to connect 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** during creation.

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

5 Configuring a VPC Endpoint for Accessing the Private IP Address of OBS over Private Networks

5.1 Overview

Scenarios

If you want to access a cloud service like OBS from an on-premises data center, 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.

Figure 5-1 Accessing OBS (private address) from an on-premises data center

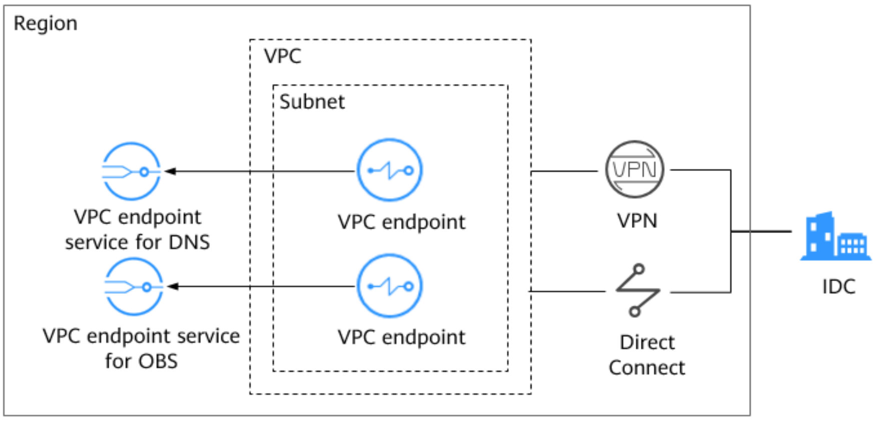


Figure 5-1 shows the process of connecting the on-premise data center to a VPC over VPN or Direct Connect, and then using two VPC endpoints to access DNS and OBS, respectively.

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.

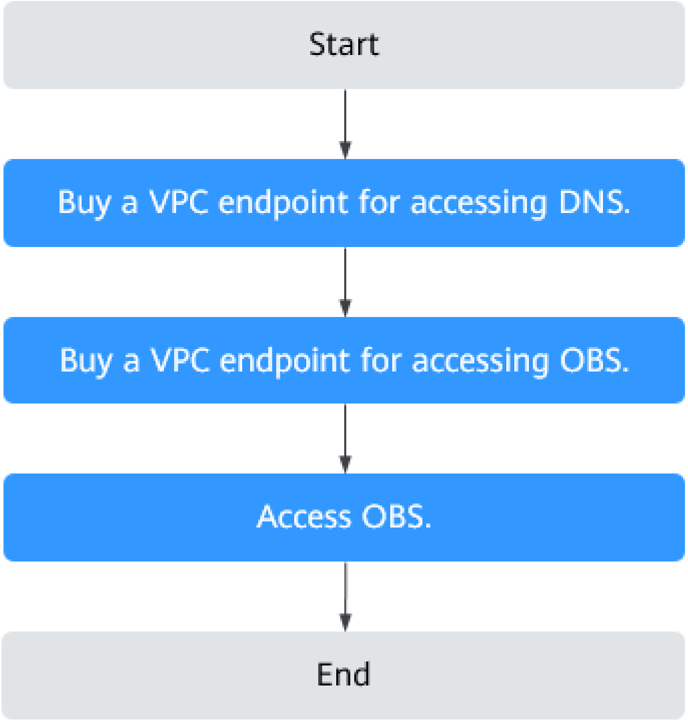
The following VPC endpoint services are required:

- VPC endpoint service for DNS: resolves the OBS domain name at the on-premises data center.
- VPC endpoint service for OBS: provides the OBS service for the on-premises data center.

Configuration Process

Figure 5-2 shows the process for configuring a VPC endpoint to access OBS (private address) from the on-premises data center.

Figure 5-2 Configuration flowchart


Start
Buy a VPC endpoint for accessing DNS.
Buy a VPC endpoint for accessing OBS.
Access OBS.
End

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 is available.

Procedure

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

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

5. Configure VPC endpoint parameters.

Table 5-1 VPC endpoint parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint 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.
Billing Mode	Specifies the billing mode of the VPC endpoint. VPC endpoints can be used or deleted at any time. VPC endpoints support only pay-per-use billing based on the usage duration.
Service Category	There are two options: ● **Cloud services**: Select this value if the target VPC endpoint service is a cloud service. ● **Find a service by name**: Select this value if the target VPC endpoint service is a private service of your own. In this example, select **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 the O&M personnel and you can directly use it. In this example, select **eu.myhuaweicloud.eu-west-101.dns**.
Create a Private Domain Name	If you want to access a VPC endpoint using a domain name, select **Create a Private Domain Name** when buying a VPC endpoint. 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.

Parameter	Description
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 deployed.
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 **Automatically assign** or **Manually specify**.
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 and CIDR blocks that are allowed to access the VPC endpoint. ● If **Access Control** is enabled, only IP addresses or CIDR blocks in the whitelist are allowed to access the VPC endpoint. ● If **Access Control** is disabled, any IP address or CIDR block can access the VPC endpoint.
Whitelist	This parameter is available 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 up to 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 characters. ● Cannot start or end with a space or contain special characters =*<>\,|/
Tag value	● Cannot be left blank. ● Can contain a maximum of 43 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 **eu.myhuaweicloud.eu-west-101.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 assigned together with a private domain name if you select **Create a Private Domain Name** during creation.

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 on-premises data center.

Prerequisites

The required VPC endpoint service is available.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the required region and project.
3. Click **Service List** and choose **Networking** > **VPC Endpoint**.

4. On the **VPC Endpoints** page, click **Buy VPC Endpoint**.

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

5. Configure VPC endpoint parameters.

Table 5-3 VPC endpoint parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint is to be located. Resources in different regions cannot communicate with each other over an intranet. For lower latency and quicker access, select the nearest region.
Billing Mode	Specifies the billing mode of the VPC endpoint. VPC endpoints can be used or deleted at any time. VPC endpoints support only pay-per-use billing based on the usage duration.
Service Category	There are two options: ● **Cloud services**: Select this value if the target VPC endpoint service is a cloud service. ● **Find a service by name**: Select this value if the target VPC endpoint service is a private service of your own. In this example, select **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 the O&M personnel and you can directly use it.
VPC	Specifies the VPC where the VPC endpoint is to be 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 to be located. For details about how to add a route, see **Adding a Custom Route** in the *Virtual Private Cloud User Guide*.

Parameter	Description
Tag	This parameter is optional. Specifies the VPC endpoint tag, which consists of a key and a value. You can add up to 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**.

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 characters. ● Cannot start or end with a space or contain special characters =*<>\,|/
Tag value	● Cannot be left blank. ● Can contain a maximum of 43 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 the VPC endpoint service for OBS is created.
8. In the VPC endpoint list, click the ID of the target VPC endpoint to view its details.

5.4 Step 3: Access OBS

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 on-premises data center over 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 the ***Virtual Private Network User Guide***.
- The VPC subnet that needs to communicate with the on-premises data center over the Direct Connect 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 target VPC endpoint and click the ID of the endpoint to view its details.
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.

```
zone "obs.xxxx.myhuaweicloud.com" {
type forward;
forward only;
forwarders{ xx.xx.xx.xx;};
};
zone "obs.xxxx.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 IP address obtained in **1**.

3. Configure a DNS route from your on-premises data center to the VPN gateway or Direct Connect 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 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 format corresponding to the actual OS.

4. Configure an OBS route from the on-premises 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 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 bucket.endpoint
   ```

   In the command:

   – *bucket*: indicates the bucket name.

   – *endpoint*: indicates the OBS endpoint.