

VPC Endpoint

User Guide

Issue 01
Date 2020-07-31



Copyright © Huawei Technologies Co., Ltd. 2021. 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 Service Overview	1
1.1 What Is VPC Endpoint?	1
1.2 Product Advantages	3
1.3 Application Scenarios	3
1.4 Constraints	5
1.5 VPCEP and Other Services	5
1.6 Permission Management	6
1.7 Product Concepts	8
1.7.1 VPC Endpoint Services	8
1.7.2 VPC Endpoints	9
1.7.3 User Permissions	10
1.7.4 Region and AZ	10
2 Getting Started	12
2.1 Operation Guide	12
2.2 Configuring a VPC Endpoint for Communication Across VPCs of the Same Domain	13
2.2.1 Overview	13
2.2.2 Step 1: Create a VPC Endpoint Service	14
2.2.3 Step 2: Create a VPC Endpoint	17
2.3 Configuring a VPC Endpoint for Communication Across VPCs of Different Domains	20
2.3.1 Overview	20
2.3.2 Step 1: Create a VPC Endpoint Service	21
2.3.3 Step 2: Add a Whitelist Record	24
2.3.4 Step 3: Create a VPC Endpoint	25
2.4 Configuring a VPC Endpoint for Accessing OBS Using the OBS Private Address	27
2.4.1 Overview	27
2.4.2 Step 1: Create a VPC Endpoint for Connecting to DNS	28
2.4.3 Step 2: Create a VPC Endpoint for Connecting to OBS	31
2.4.4 Step 3: Access OBS	32
3 VPC Endpoint Services	35
3.1 VPC Endpoint Service Overview	35
3.2 Creating a VPC Endpoint Service	37
3.3 Viewing Summary of a VPC Endpoint Service	40

3.4 Deleting a VPC Endpoint Service.....	43
3.5 Managing Connections of a VPC Endpoint Service.....	43
3.6 Managing Whitelist Records of a VPC Endpoint Service.....	44
3.7 Viewing Port Mappings of a VPC Endpoint Service.....	45
3.8 Managing Tags of a VPC Endpoint Service.....	46
4 VPC Endpoints.....	49
4.1 VPC Endpoint Overview.....	49
4.2 Creating a VPC Endpoint.....	50
4.3 Querying and Accessing a VPC Endpoint.....	53
4.4 Deleting a VPC Endpoint.....	56
4.5 Managing Tags of a VPC Endpoint.....	56
5 Permission Management.....	59
5.1 Creating a User and Granting Permissions.....	59
6 FAQs.....	61
6.1 What Is a Quota?.....	61
6.2 How Can I Check Network Configurations of the ECS Hosting the VPC Endpoint Service?.....	61
6.3 What Are the Differences Between VPC Endpoints and VPC Peering Connections?.....	62
6.4 What Are Statuses of VPC Endpoint Services and VPC Endpoints?.....	63
A Change History.....	65

1 Service Overview

1.1 What Is VPC Endpoint?

VPC Endpoint (VPCEP) is a cloud service that provides secure and private channels to connect your VPCs to VPC endpoint services, including cloud services or your private services. It allows you to plan networks flexibly without having to use EIPs.

Architecture

There are two types of resources: VPC endpoint services and VPC endpoints.

- VPC endpoint services are cloud services or private services that you manually configure in VPCEP. You can access these endpoint services using VPC endpoints.
For more information, see [VPC Endpoint Services](#).
- VPC endpoints are secure and private channels for connecting VPCs to VPC endpoint services.
For more information, see [VPC Endpoints](#).

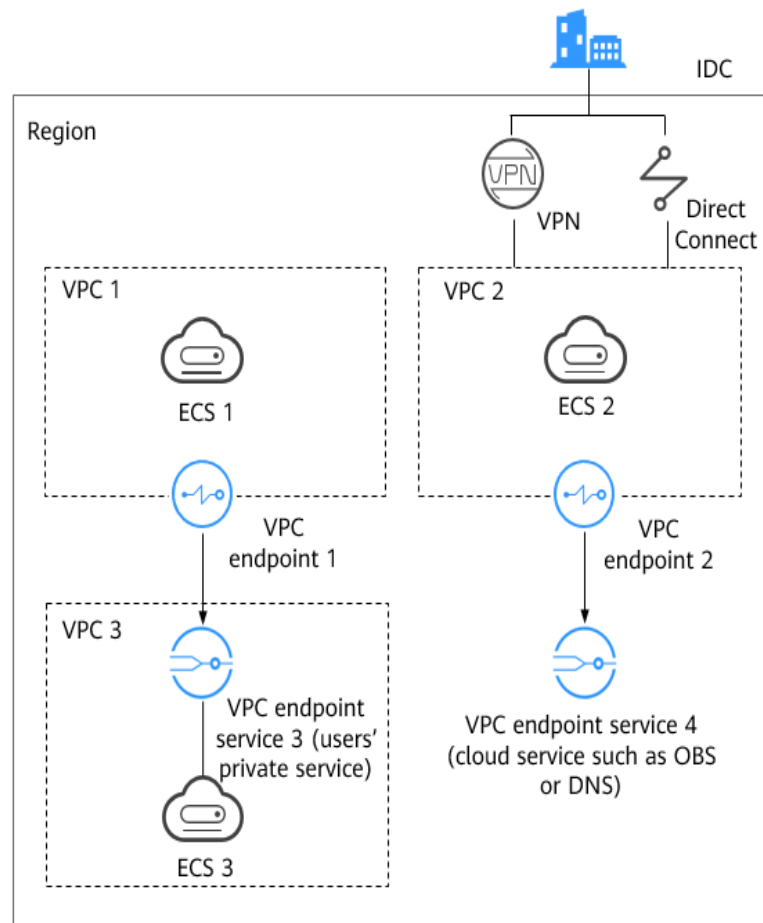
Figure 1-1 How VPCEP works

Figure 1-1 shows the process of establishing channels for network communications between:

- VPC 1 (ECS 1) and VPC 3 (ECS 3)
- VPC 2 (ECS 2) and cloud services such as OBS and DNS
- IDC and VPC 2 over VPN or Direct Connect to finally access a cloud service such as OBS or DNS

For more information, see [Application Scenarios](#).

Accessing VPCEP

A web-based console and HTTPS APIs are provided for you to access VPCEP.

- Web-based console

You can access VPCEP using the web-based console.

Upon a quick configuration on the management console, you can start using VPCEP.

- APIs

Access VPCEP using an API if you need to integrate VPCEP with a third-party system for secondary development. For details, see *VPC Endpoint API Reference*.

1.2 Product Advantages

- **Excellent Performance:** Each gateway supports up to 1 million concurrent connections in a variety of application scenarios.
- **Immediately Ready for Use Upon Creation:** VPC endpoints take effect a few seconds after they are created.
- **Easy to Use:** You can use VPC endpoints to access resources over private networks, without having to use EIPs.
- **High Security:** VPC endpoints enable you to access VPC endpoint services without exposing server information, minimizing security risks.

1.3 Application Scenarios

VPCEP establishes a secure and private channel between a VPC endpoint (cloud resources in a VPC) and a VPC endpoint service in the same region.

You can use VPCEP in different scenarios.

High-Speed Access to Cloud Services

After you connect an IDC to a VPC using VPN or Direct Connect, you can use a VPC endpoint to connect the VPC to a cloud service or one of your private services, so that the IDC can access the cloud service or private service.

Figure 1-2 Access to cloud services

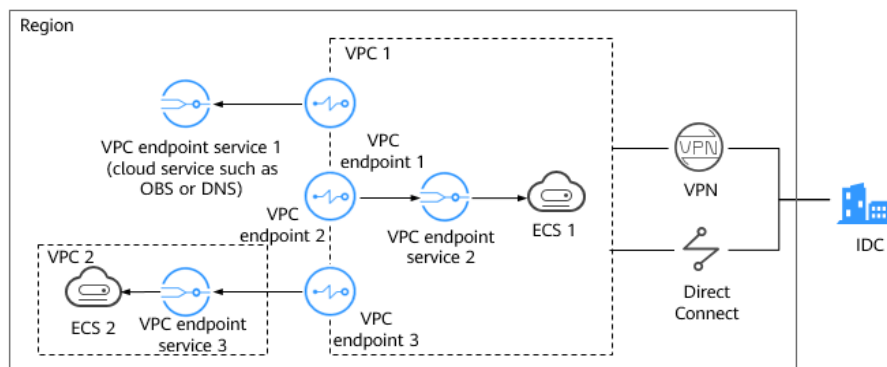


Figure 1-2 shows the process of connecting an IDC to VPC 1 over VPN or Direct Connect, for the purpose of:

- Accessing OBS or DNS using VPC endpoint 1
- Accessing ECS 1 in the same VPC using VPC endpoint 2
- Accessing ECS 2 in VPC 2 using VPC endpoint 3

For cloud migration, VPCEP has the following advantages:

- Simple and efficient
The IDC is directly connected to the VPC endpoint service over a private network, reducing access latency and improving efficiency.
- Low cost
With VPCEP, your IDC can access cloud resources over a private network, reducing your costs on public resources.

For details, see [Configuring a VPC Endpoint for Accessing OBS Using the OBS Private Address](#).

Cross-VPC Connection

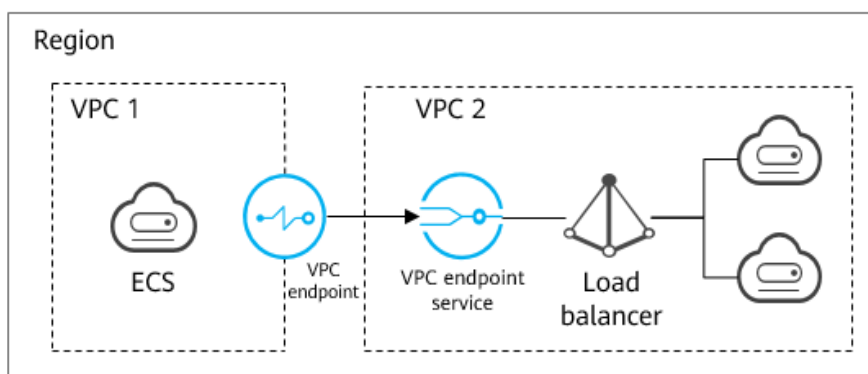
With VPCEP, resources in two different VPCs can communicate with each other despite of logic isolation between them as long as the two VPCs are in the same region.

NOTE

VPC endpoints and VPC peering connections are different in security, communication methods, route configurations, and more.

For details, see [What Are the Differences Between VPC Endpoints and VPC Peering Connections?](#)

Figure 1-3 Cross-VPC connection



An ECS in VPC 1 uses a VPC endpoint to access a load balancer in VPC 2 over a private network. **Figure 1-3** shows the connection process.

VPCEP has the following advantages:

- High performance
Each gateway supports up to 1 million concurrent connections.
- Simplified operations
VPCEP resources can be created within seconds and take effect quickly.

For details, see the following sections:

- [Configuring a VPC Endpoint for Communication Across VPCs of the Same Domain](#)

- [Configuring a VPC Endpoint for Communication Across VPCs of Different Domains](#)

1.4 Constraints

Constraints on Resource Quotas

[Table 1-1](#) describes constraints on the VPCEP resource quota.

Table 1-1 VPCEP resource quotas

Resource	Quota	How to Increase Quota
VPC endpoint services per account	20	What Is a Quota?
VPC endpoints per account	50	

Other Constraints

- When you create a VPC endpoint, ensure that the associated VPC endpoint service has been created and is in the same region as the VPC endpoint.
- One VPC endpoint can be used to connect to only one VPC endpoint service.
- A VPC endpoint supports a maximum of 3000 concurrent requests.
- One VPC endpoint service can be connected by multiple VPC endpoints.
- One VPC endpoint service corresponds to only one backend resource.

1.5 VPCEP and Other Services

[Table 1-2](#) shows the relationship between VPCEP and other cloud services.

Table 1-2 Relationships with other services

Interactive Function	Service	Reference
Creating VPC endpoint services for resources in your VPC	VPC	<ul style="list-style-type: none">• Configuring a VPC Endpoint for Communication Across VPCs of the Same Domain• Configuring a VPC Endpoint for Communication Across VPCs of Different Domains

Interactive Function	Service	Reference
Connecting an IDC to your VPC using a VPN connection and connecting your VPC to a cloud service through VPCEP	VPN	Configuring a VPC Endpoint for Accessing OBS Using the OBS Private Address
Connecting an IDC to your VPC using a direct connection and connecting your VPC to a cloud service through VPCEP	Direct Connect	
When an enterprise needs to provide VPCEP for multiple users, the enterprise administrator can use IAM to create users and control access of these domains to enterprise resources.	IAM	-
Configured as a gateway VPC endpoint service by default. You can create a VPC endpoint to access the VPC endpoint service.	OBS	Creating a VPC Endpoint
Configured as an interface VPC endpoint service by default. You can create VPC endpoints to access these endpoint services.	DNS	Creating a VPC Endpoint
Configuring a private service as a VPC endpoint service. You can create a VPC endpoint to access the VPC endpoint service.	Load balancer	Creating a VPC Endpoint Service
	ECS	

1.6 Permission Management

If you need to assign different permissions to employees in your enterprise to access your cloud resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your cloud services.

With IAM, you can use your account to create IAM users for your employees, and assign permissions to the users to control their access to specific cloud service resources. For example, you need to allow website maintenance personnel in your enterprise to use VPCEP resources but do not want them to delete other cloud resources or perform any high-risk operations. To achieve this result, you can create IAM users for the maintenance personnel and grant them only the permissions required for using VPCEP resources.

If you do not need to create IAM users in your account for permissions management, you may skip over this section.

IAM is free of charge. You pay only for the resources in your account.

For more information, see [IAM Service Overview](#).

VPCEP Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

VPCEP is a project-level service deployed and accessed in specific physical regions. To assign SMN permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing the VPCEP service, users need to switch to a region where they have been authorized to use VPCEP resources.

[Table 1-3](#) lists all system-defined roles supported by VPCEP.

Table 1-3 System-defined roles supported by VPCEP

System-defined Role	Description	Category	Dependency
VPCEP Administrator	Full permissions for VPCEP	System-defined role	This role depends on Server Administrator , VPC Administrator , and DNS Administrator roles in the same project.

[Table 1-4](#) lists the common operations for each system-defined policy or role of VPCEP. Select policies or roles as needed.

Table 1-4 Common operations supported by the VPCEP system policies

Operation	VPCEP Administrator
Creating a VPC endpoint	Yes

Operation	VPC Endpoint Administrator
Deleting a VPC endpoint	Yes
Querying a VPC endpoint	Yes
Modifying a VPC endpoint	Yes
Creating a VPC endpoint service	Yes
Deleting a VPC endpoint service	Yes
Querying a VPC endpoint service	Yes
Modifying a VPC endpoint service	Yes

Helpful Links

- [IAM Service Overview](#)
- [Creating a User and Granting Permissions](#)

1.7 Product Concepts

1.7.1 VPC Endpoint Services

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

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

- Gateway VPC endpoint services are created only for cloud services.
- Interface VPC endpoint services can be created for both cloud services and your private services. All VPC endpoint services for cloud services are created by default while those for private services need to be created by users themselves.

Gateway VPC Endpoint Services

Gateway endpoint services are configured from cloud services by the system. You do not have the permission to configure such services but can select them when creating a VPC endpoint.

NOTE

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

Table 1-5 Supported gateway VPC endpoint services

VPC Endpoint Service	Category	Type	Example	Description
OBS	Cloud service	Gateway	None	Access OBS using its private address.

Interface VPC Endpoint Services

Interface VPC endpoint services are mainly configured from:

- Cloud services. You do not have the permission to configure such endpoint services, but can select them when they create a VPC endpoint.
- Your private services

 **NOTE**

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

Table 1-6 Supported interface VPC endpoint services

VPC Endpoint Service	Category	Type	Example	Description
DNS	Cloud service	Interface	None	VPC endpoint services enable you to access DNS over private networks.
Load balancer	Users' private service	Interface	None	Select a load balancer as the backend resource if your services receive high traffic and demand high reliability and disaster recovery (DR) performance.
ECS	Users' private service	Interface	None	VPC endpoint services work as servers.

1.7.2 VPC Endpoints

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

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

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

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

1.7.3 User Permissions

The cloud system provides two types of user permissions by default, user management and resource management.

- User management refers to management of users, user groups, and user group permissions.
- Resource management refers to access control over cloud service resources.

VPCEP provides two types of resources: VPC endpoint services and VPC endpoints, both of which are region-level resources. The required permissions must be added for users in the project.

1.7.4 Region and AZ

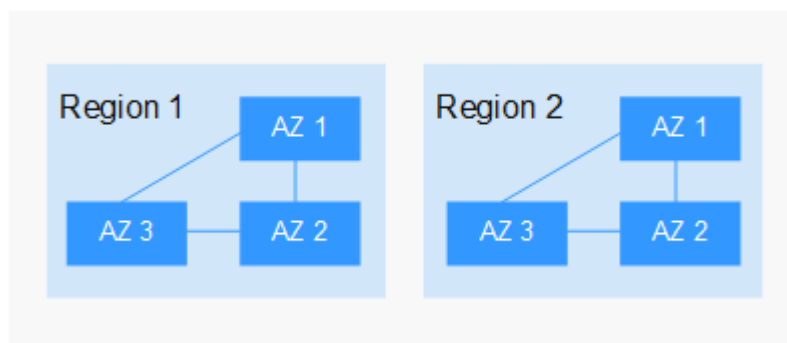
Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.
- An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in one AZ will not affect others.

Figure 1-4 shows the relationship between regions and AZs.

Figure 1-4 Regions and AZs



Selecting a Region

Select a region closest to your target users for lower network latency and quick access.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

2 Getting Started

2.1 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 2-1](#).

Table 2-1 Application scenarios

Scenario	Description
Communication between cloud resources across VPCs in the same region	You can create a VPC endpoint service and a VPC endpoint to access cloud services across VPCs. For details, see the following sections: <ul style="list-style-type: none">• Configuring a VPC Endpoint for Communication Across VPCs of the Same Domain• Configuring a VPC Endpoint for Communication Across VPCs of Different Domains
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

2.2 Configuring a VPC Endpoint for Communication Across VPCs of the Same Domain

2.2.1 Overview

Scenarios

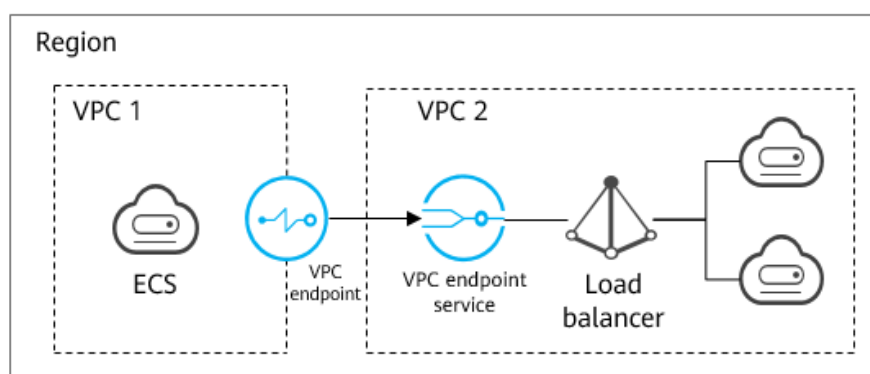
With VPCEP, you can access resources across VPCs in the same region.

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 domains. This section uses the communication across two VPCs of the same domain as an example.

For example, VPC 1 and VPC 2 belong to the same domain. Configure a load balancer in VPC 2 as a VPC endpoint service and create 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 2-1 Cross-VPC communication

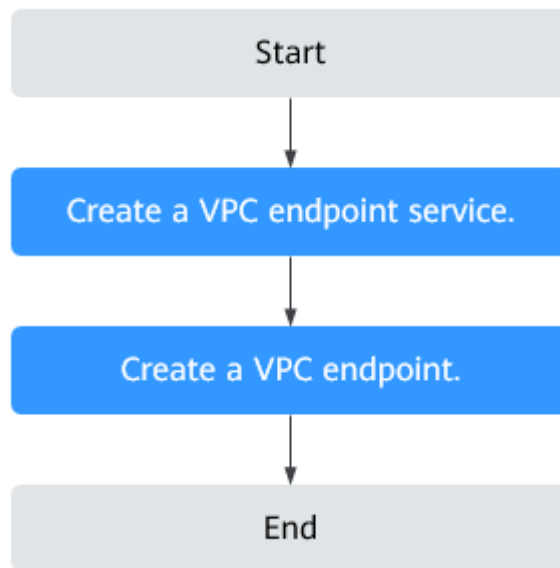


NOTE

- Only one-way communication from the VPC endpoint to the VPC endpoint service is supported.
- For details about communication between two VPCs of different domains, see [Configuring a VPC Endpoint for Communication Across VPCs of Different Domains](#).

Configuration Process

Figure 2-2 shows how to enable network communication between two VPCs of the same domain using VPCEP.

Figure 2-2 Cross-VPC communication

2.2.2 Step 1: Create a VPC Endpoint Service

Scenarios

To enable communication 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.
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.
5. Set the required parameters.

Table 2-2 Required parameters

Parameter	Description
Region	<p>Specifies the region where the VPC endpoint service is located.</p> <p>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.</p>
VPC	Specifies the VPC where the VPC endpoint service is located.
Service Type	Specifies the type of the VPC endpoint service. The value can only be Interface .
Connection Approval	<p>Specifies whether the connection between a VPC endpoint and a VPC endpoint service requires approval from the owner of the VPC endpoint service.</p> <p>You can determine whether to enable or disable the connection approval.</p> <p>If connection approval is enabled, any VPC endpoint for connecting to the VPC endpoint service needs to be approved. For details, see step 7.</p>
Port Mapping	<p>Specifies the protocol and ports used for communication between the VPC endpoint service and VPC endpoint. The protocol is TCP.</p> <ul style="list-style-type: none">• 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. <p>The service and terminal port numbers range from 1 to 65535. A maximum of 50 port mappings can be added at a time.</p> <p>NOTE Accessing a VPC endpoint service from a VPC endpoint is to access the service port from the associated terminal port.</p>

Parameter	Description
Backend Resource Type	<p>Specifies the type of the backend resource that provides services to be accessed.</p> <p>The following backend resources are supported:</p> <ul style="list-style-type: none"> • Elastic load balancer: Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance. • ECS: Backend resources of this type serve as servers. <p>Example: Elastic load balancer</p> <p>NOTE Security groups use the whitelist mechanism. For the security group containing the backend resource configured for the VPC endpoint service, add an inbound rule, with the source IP address set to 198.19.128.0/20. For details, see section "Adding a Security Group Rule" in the <i>Virtual Private Cloud User Guide</i>.</p>
Load Balancer	<p>When Backend Resource Type is set to Elastic load balancer, select the load balancer that provides services from the drop-down list.</p> <p>NOTE If an elastic load balancer is used as the backend resource, the source IP address received by the VPC endpoint service is not the real address of the client.</p>
Tag	<p>This parameter is optional.</p> <p>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.</p> <p>Tag keys and values must meet requirements listed in Table 2-3.</p>

Table 2-3 Tag requirements for VPC endpoint services

Parameter	Requirement
Tag key	<ul style="list-style-type: none"> • Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 36 Unicode characters. • Cannot start or end with a space or contain special characters =*<>\\, /
Tag value	<ul style="list-style-type: none"> • 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.

2.2.3 Step 2: Create a VPC Endpoint

Scenarios

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

This section describes how to create 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 **Create VPC Endpoint**.
The **Create VPC Endpoint** page is displayed.
5. Set the required parameters.

Table 2-4 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.
Service Category	There are two options: Cloud services or Find a service by name . <ul style="list-style-type: none">● 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

Parameter	Description
VPC Endpoint Service Name	<p>This parameter is available only when you select Find a service by name for Service Category.</p> <p>Enter the VPC endpoint service name recorded in step 8 and click Verify.</p> <ul style="list-style-type: none"> • If Service name found is displayed, proceed with subsequent operations. • If Service name not found is displayed, check whether the region is the same as that of the connected VPC endpoint service or whether the entered service name is correct.
Private Domain Name	<p>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.</p> <ul style="list-style-type: none"> • 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 located.
Subnet	Specifies the subnet where the VPC endpoint is located.
Tag	<p>This parameter is optional.</p> <p>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.</p> <p>Tag keys and values must meet requirements listed in Table 2-5.</p>


Table 2-5 Tag requirements for VPC endpoints

Parameter	Requirement
Tag key	<ul style="list-style-type: none"> • Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 36 Unicode characters. • Cannot start or end with a space or contain special characters =*<>\\ /
Tag value	<ul style="list-style-type: none"> • 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 **Create Now**.
 - 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  before 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**.

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.

Figure 2-3 Logging in to the 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 ██████ 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+0a j0+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
```

2.3 Configuring a VPC Endpoint for Communication Across VPCs of Different Domains

2.3.1 Overview

Scenarios

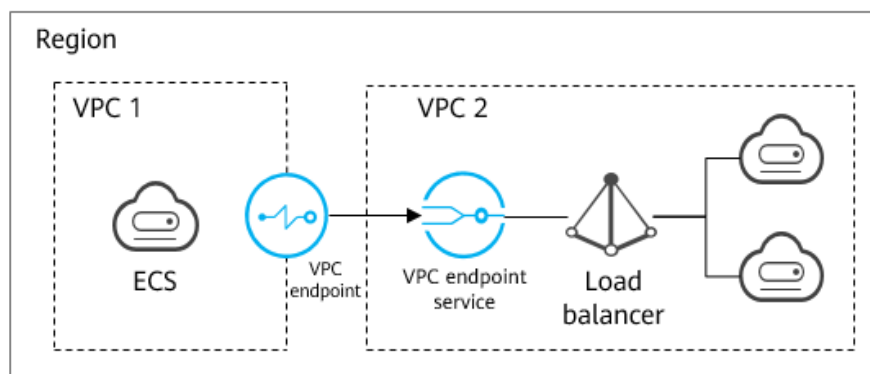
With VPCEP, you can access resources across VPCs in the same region.

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 domains. This section focuses on the communication across two VPCs of different domains.

For example, VPC 1 and VPC 2 belong to different domains A and B, respectively. Configure a load balancer in VPC 2 as a VPC endpoint service and create 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 2-4 Cross-VPC communication

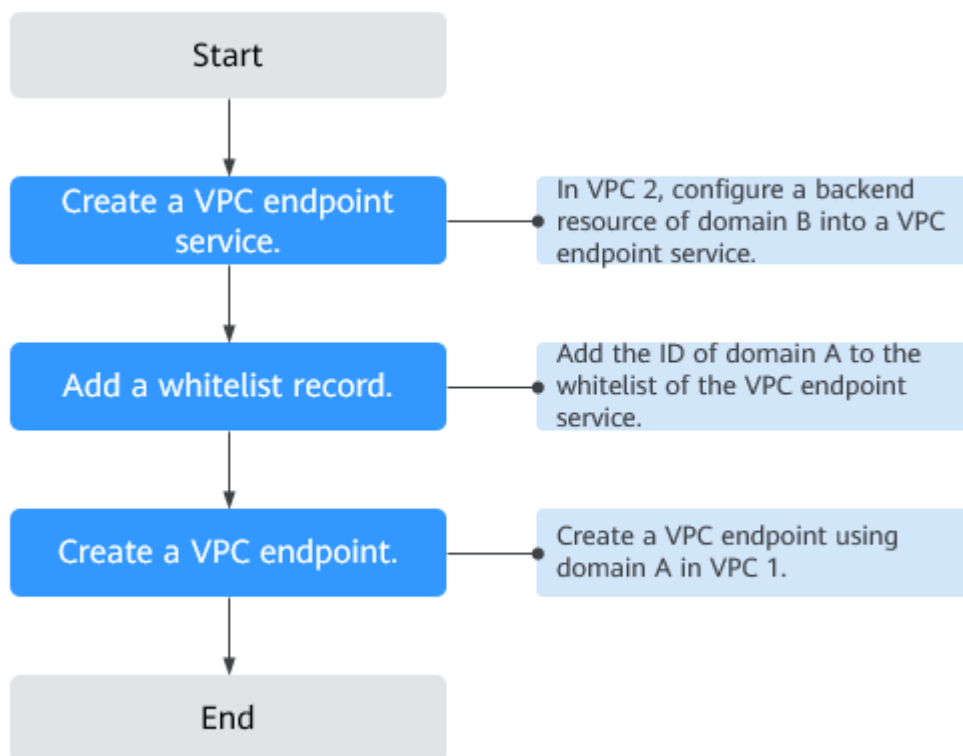


NOTE

- Only one-way communication from the VPC endpoint to the VPC endpoint service is supported.
- Before you create a VPC endpoint, add the authorized domain ID of VPC 1 to the whitelist of the VPC endpoint service in VPC 2.
- For details about communication between two VPCs of the same domain, see [Configuring a VPC Endpoint for Communication Across VPCs of the Same Domain](#).

Cross-VPC Communication

Figure 2-5 shows how to configure networks between two VPCs of different domains using VPCEP.

Figure 2-5 Cross-VPC communication flowchart

2.3.2 Step 1: Create a VPC Endpoint Service

Scenarios

To enable communication 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 domain 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. 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.
5. Set the required parameters.

Table 2-6 Required parameters

Parameter	Description
Region	<p>Specifies the region where the VPC endpoint service is located.</p> <p>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.</p>
VPC	Specifies the VPC where the VPC endpoint service is located.
Service Type	Specifies the type of the VPC endpoint service. The value can only be Interface .
Connection Approval	<p>Specifies whether the connection between a VPC endpoint and a VPC endpoint service requires approval from the owner of the VPC endpoint service.</p> <p>You can determine whether to enable or disable the connection approval.</p> <p>If connection approval is enabled, any VPC endpoint for connecting to the VPC endpoint service needs to be approved. For details, see step 7.</p>
Port Mapping	<p>Specifies the protocol and ports used for communication between the VPC endpoint service and VPC endpoint. The protocol is TCP.</p> <ul style="list-style-type: none">• 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. <p>The service and terminal port numbers range from 1 to 65535. A maximum of 50 port mappings can be added at a time.</p> <p>NOTE Accessing a VPC endpoint service from a VPC endpoint is to access the service port from the associated terminal port.</p>

Parameter	Description
Backend Resource Type	<p>Specifies the type of the backend resource that provides services to be accessed.</p> <p>The following backend resources are supported:</p> <ul style="list-style-type: none"> • Elastic load balancer: Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance. • ECS: Backend resources of this type serve as servers. <p>Example: Elastic load balancer</p> <p>NOTE Security groups use the whitelist mechanism. For the security group containing the backend resource configured for the VPC endpoint service, add an inbound rule, with the source IP address set to 198.19.128.0/20. For details, see section "Adding a Security Group Rule" in the <i>Virtual Private Cloud User Guide</i>.</p>
Load Balancer	<p>When Backend Resource Type is set to Elastic load balancer, select the load balancer that provides services from the drop-down list.</p> <p>NOTE If an elastic load balancer is used as the backend resource, the source IP address received by the VPC endpoint service is not the real address of the client.</p>
Tag	<p>This parameter is optional.</p> <p>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.</p> <p>Tag keys and values must meet requirements listed in Table 2-7.</p>

Table 2-7 Tag requirements for VPC endpoint services

Parameter	Requirement
Tag key	<ul style="list-style-type: none"> • Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 36 Unicode characters. • Cannot start or end with a space or contain special characters =*<>\\, /
Tag value	<ul style="list-style-type: none"> • 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.

2.3.3 Step 2: Add a Whitelist Record

Scenarios

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

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

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


Prerequisites

The target VPC endpoint service already exists.

Obtain the ID of Your Own Domain

1. Log in to the management console.
2. Click **My Credentials** under the domain.
The **My Credentials** page is displayed. You can view the Domain ID of VPC 1.

Add an Authorized Domain 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 domain ID in the required format and click **OK**.

NOTE

- Your domain is in the whitelist of your VPC endpoint service by default.
 - The authorized domain ID is in the **iam:domain::domain_id** format.
domain_id indicates the ID of the authorized domain, for example, **iam:domain::1564ec50ef2a47c791ea5536353ed4b9**
 - Adding * to the whitelist means that all users can access the VPC endpoint service.
8. Click **OK**.

2.3.4 Step 3: Create a VPC Endpoint

Scenarios

After you add the required whitelist record, you can create 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. Choose **Service List > Networking > VPC Endpoint**.
4. On the **VPC Endpoints** page, click **Create VPC Endpoint**.
The **Create VPC Endpoint** page is displayed.
5. Set the required parameters.

Table 2-8 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.
Service Category	There are two options: Cloud services or Find a service by name . <ul style="list-style-type: none">● 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 . <ul style="list-style-type: none">● If Service name found is displayed, proceed with subsequent operations.● If Service name not found is displayed, check whether the region is the same as that of the connected VPC endpoint service or whether the entered service name is correct.

Parameter	Description
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. <ul style="list-style-type: none"> 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 located.
Subnet	Specifies the subnet where the VPC endpoint is located.
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 2-9 .


Table 2-9 Tag requirements for VPC endpoints

Parameter	Requirement
Tag key	<ul style="list-style-type: none"> Cannot be left blank. Must be unique for each resource. Can contain a maximum of 36 Unicode characters. Cannot start or end with a space or contain special characters =* <> \, /
Tag value	<ul style="list-style-type: none"> 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 **Create Now**.
 - 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  before 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**.

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

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

2.4.1 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.

Figure 2-6 Accessing OBS using its private address from an IDC

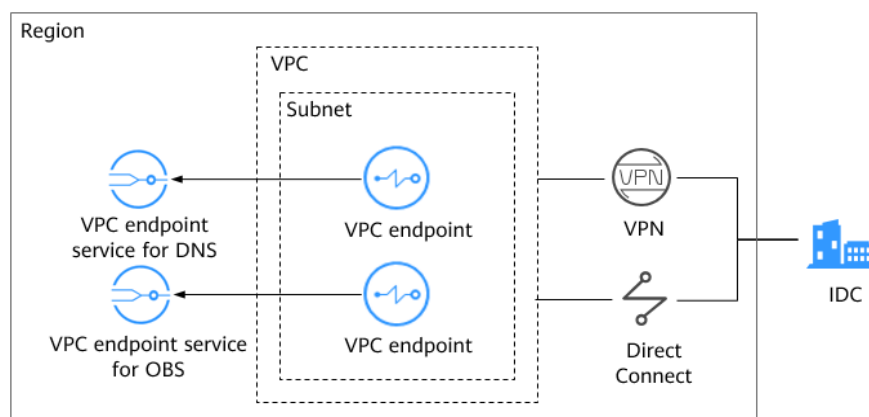


Figure 2-6 shows the process of connecting an IDC to a VPC over VPN or Direct Connect to access DNS and OBS using two VPC endpoints, respectively.

A VPC endpoint comes with a VPC endpoint service. Before you create a VPC endpoint, ensure that the target VPC endpoint service is available.

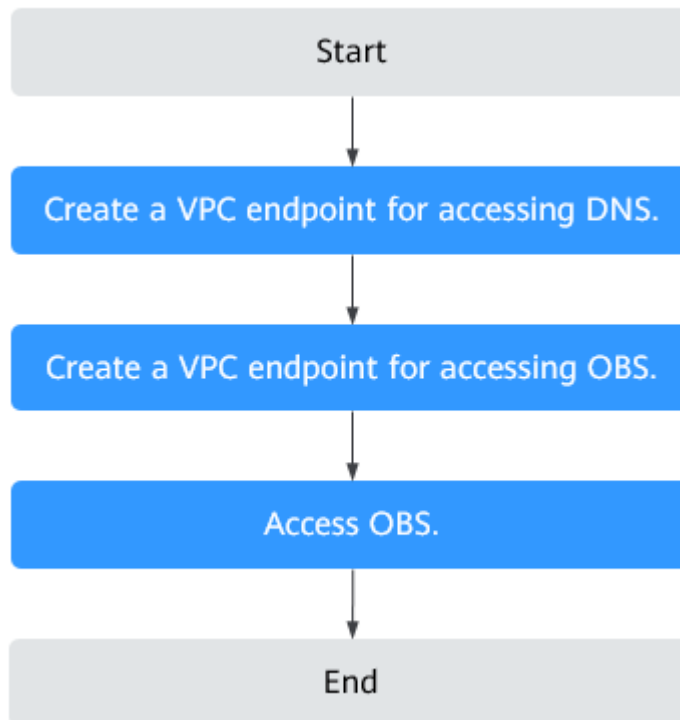
The following VPC endpoint services are required:

- VPC endpoint service for DNS: resolves the OBS domain name at the IDC.
- VPC endpoint service for OBS: provides the OBS service for the IDC.

Configuration Process

Figure 2-7 shows the process for configuring a VPC endpoint to access OBS using its private address from an IDC.

Figure 2-7 Configuration flowchart



2.4.2 Step 1: Create a VPC Endpoint for Connecting to DNS

Scenarios

This section describes how to create 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.

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 **Create VPC Endpoint**.
The **Create VPC Endpoint** page is displayed.
5. Set the required parameters.


Table 2-10 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.
Service Category	There are two options: Cloud services or Find a service by name . <ul style="list-style-type: none">● Cloud services: Select this value if the target VPC endpoint service is a cloud service.● Find a service by name: Select this value if the target VPC endpoint service is a private service of your own. 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. Select the VPC endpoint service for 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: <ul style="list-style-type: none">● 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 located.

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 located.
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 2-11 .

Table 2-11 Tag requirements for VPC endpoints

Parameter	Requirement
Tag key	<ul style="list-style-type: none"> • Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 36 Unicode characters. • Cannot start or end with a space or contain special characters =*<>\\ /
Tag value	<ul style="list-style-type: none"> • 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 **Create Now**.
 - 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 the VPC endpoint service for DNS is created.
8. In the VPC endpoint list, click  before 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.

2.4.3 Step 2: Create a VPC Endpoint for Connecting to OBS

Scenarios

This section describes how to create 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 **Create VPC Endpoint**.
The **Create VPC Endpoint** page is displayed.
5. Set the required parameters.


Table 2-12 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.
Service Category	There are two options: Cloud services or Find a service by name . <ul style="list-style-type: none">• Cloud services: Select this value if the target VPC endpoint service is a cloud service.• Find a service by name: Select this value if the target VPC endpoint service is a private service of your own. 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. Select the VPC endpoint service for OBS.
VPC	Specifies the VPC where the VPC endpoint is located.

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 2-13 .

Table 2-13 Tag requirements for VPC endpoints

Parameter	Requirement
Tag key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each resource.• Can contain a maximum of 36 Unicode characters.• Cannot start or end with a space or contain special characters =*<>\\ /
Tag value	<ul style="list-style-type: none">• 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 **Create Now**.
 - 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  before the target VPC endpoint to view its details.

2.4.4 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 the *Virtual Private Network User Guide*.
- The CIDR block of the virtual gateway associated with your direct connection contains the OBS CIDR block 100.125.0.0/16.
For details about how to enable Direct Connect, see the *Direct Connect User Guide*.

Procedure

1. In the VPC endpoint list, locate the target VPC endpoint and click  before 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:

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};  
};
```

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
```

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.ap-southeast-1.myhuaweicloud.com***

 **NOTE**

Obtain OBS endpoint information at [Regions and Endpoints](#).

3 VPC Endpoint Services

3.1 VPC Endpoint Service Overview

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

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

- Gateway VPC endpoint services are created only for cloud services.
- Interface VPC endpoint services can be created for both cloud services and your private services. All VPC endpoint services for cloud services are created by default while those for private services need to be created by users themselves.

NOTE

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

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

Table 3-1 Management of VPC endpoint services

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

Operation	Description	Constraint
Managing Connections of a VPC Endpoint Service	Describes how to set connection approval of a VPC endpoint service to determine whether to allow a VPC endpoint to connect to the VPC endpoint service.	You can specify whether to allow a VPC endpoint to connect to a VPC endpoint service only when connection approval is enabled during VPC endpoint service creation.
Managing Whitelist Records of a VPC Endpoint Service	Describes how to manage whitelist records of a VPC endpoint service to control across-account access between a VPC endpoint and a VPC endpoint service.	<ul style="list-style-type: none"> The VPC endpoint must be in the same region as the VPC endpoint service. Before you configure the whitelist for a VPC endpoint service, obtain the domain ID of the associated VPC endpoint.
Viewing Port Mappings of a VPC Endpoint Service	Describes how to view the port mapping between a VPC endpoint and a VPC endpoint service, including the supported protocol, service port, and terminal port.	<ul style="list-style-type: none"> Configuring a port mapping is required when you create a VPC endpoint service. After a VPC endpoint service is created, you can view its port mappings but cannot modify them.
Managing Tags of a VPC Endpoint Service	Describes how to manage VPC endpoint service tags, including viewing, adding, editing, and deleting tags.	A maximum of 10 tags can be added to each VPC endpoint service.

3.2 Creating a VPC Endpoint Service

Scenarios

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

- Gateway VPC endpoint services are created only for cloud services.
- Interface VPC endpoint services can be created for both cloud services and your private services. All VPC endpoint services for cloud services are created by default while those for private services need to be created by users themselves.

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

Constraints

- VPC endpoint services are region-level resources. Select a region and project when you create such a service.
- Each tenant can create a maximum of 20 VPC endpoint services.

- The following private services can be configured into VPC endpoint services:
 - **Elastic load balancer:** Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance.
 - **ECS:** Backend resources of this type serve as servers.
- One VPC endpoint service corresponds to only one backend resource.

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. 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.
5. Configure parameters by referring to [Table 3-2](#).

Table 3-2 Required parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint service 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.
VPC	Specifies the VPC where the VPC endpoint service is located.
Service Type	Specifies the type of the VPC endpoint service. The value 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 Managing Connections of a VPC Endpoint Service .

Parameter	Description
Port Mapping	<p>Specifies the protocol and ports used for communication between the VPC endpoint service and VPC endpoint. The protocol is TCP.</p> <ul style="list-style-type: none"> • 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. <p>The service and terminal port numbers range from 1 to 65535. A maximum of 50 port mappings can be added at a time.</p> <p>NOTE Accessing a VPC endpoint service from a VPC endpoint is to access the service port from the associated terminal port. After a port mapping is added, it cannot be modified or deleted.</p>
Backend Resource Type	<p>Specifies the type of the backend resource that provides services to be accessed.</p> <p>The following backend resources are supported:</p> <ul style="list-style-type: none"> • Elastic load balancer: Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance. • ECS: Backend resources of this type serve as servers. <p>Example: Elastic load balancer</p> <p>NOTE Security groups use the whitelist mechanism. For the security group containing the backend resource configured for the VPC endpoint service, add an inbound rule, with the source IP address set to 198.19.128.0/20. For details, see section "Adding a Security Group Rule" in the <i>Virtual Private Cloud User Guide</i>.</p>
Load Balancer	<p>When Backend Resource Type is set to Elastic load balancer, select the load balancer that provides services from the drop-down list.</p> <p>NOTE If an elastic load balancer is used as the backend resource, the source IP address received by the VPC endpoint service is not the real address of the client.</p>
ECS List	<p>When Backend Resource Type is set to ECS, select the ECS that provides services from the ECS list.</p>
Tag	<p>This parameter is optional.</p> <p>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.</p> <p>Tag keys and values must meet requirements listed in Table 3-3.</p>

Table 3-3 Tag requirements for VPC endpoint services

Parameter	Requirement
Tag key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each resource.• Can contain a maximum of 36 Unicode characters.• Cannot start or end with a space or contain special characters =* < > \, /
Tag value	<ul style="list-style-type: none">• 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.

3.3 Viewing Summary of a VPC Endpoint Service



Scenarios

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

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**.

Locate the target VPC endpoint service by entering a filter in the search box in the upper right corner:

- Search by name or ID.
 - i. Select **Name** or **ID** in the filter box.
 - ii. Enter a keyword in the search box.
 - iii. Click  to start the search.
VPC endpoint services containing the keyword are displayed in the list.
- Search by preset tag.
 - i. Click  in **Search by Tag**.

- ii. Enter a tag and a value.
Enter a key or value or select a key or value from the drop-down list.
You can use a maximum of 10 tags to search for a VPC endpoint service.
 - iii. Click **Search**.
The VPC endpoint service containing the specified tag is displayed in the list.
If you set multiple tags, VPC endpoint services containing all the specified tags will be displayed.
5. In the VPC endpoint service list, locate the target VPC endpoint service and click its name to view the details.

Table 3-4 describes the parameters displayed on the VPC endpoint service details page.

Table 3-4 Parameter description

Tab	Parameter	Description
Summary	Name	Specifies the name of the VPC endpoint service.
	ID	Specifies the ID of the VPC endpoint service.
	Backend Resource Type	Specifies the type of the backend resource that provides services.
	Backend Resource Name	Specifies the name of the backend resource that provides services to be accessed.
	VPC	Specifies the region where the VPC endpoint service is deployed.
	Status	Specifies the status of the VPC endpoint service.
	Connection Approval	Specifies whether connection approval is required.
	Service Type	Specifies the type of the VPC endpoint service.
	Created	Specifies the creation time of the VPC endpoint service.
Connection Management	VPC Endpoint ID	Specifies the ID of the VPC endpoint.
	Packet ID	Specifies the identifier of the VPC endpoint ID.

Tab	Parameter	Description
	Status	Specifies the status of the VPC endpoint. For details about statuses of a VPC endpoint, see What Are Statuses of VPC Endpoint Services and VPC Endpoints?
	Owner	Specifies the domain ID of the VPC endpoint owner.
	Created	Specifies the creation time of the VPC endpoint.
	Operation	Specifies whether to allow a VPC endpoint to connect to a VPC endpoint service. The value can be Accept or Reject .
Permission Management	Authorized Domain ID	Specifies the authorized domain ID for connecting to the VPC endpoint. The value can also be *. If you add an asterisk (*) to the whitelist, it means that all users can access the VPC endpoint service.
	Operation	Specifies whether to delete an authorized domain from the whitelist.
Port Mapping	Protocol	Specifies the protocol used for communication between the VPC endpoint service and VPC endpoint.
	Service Port	Specifies the port provided by the backend service bound to the VPC endpoint service.
	Terminal Port	Specifies the port provided by the VPC endpoint, allowing you to access the VPC endpoint service.
Tag	Key	Specifies the tag key of the VPC endpoint service.
	Value	Specifies the tag value of the VPC endpoint service.
	Operation	Specifies the operation on the VPC endpoint service tag, for example, you can select Edit or Delete .

3.4 Deleting a VPC Endpoint Service

Scenarios

This section describes how to delete a VPC endpoint service.

NOTE


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

Constraints

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

For statuses of a VPC endpoint, see [What Are Statuses of VPC Endpoint Services and VPC Endpoints?](#)

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**.
5. In the VPC endpoint service list, locate the target VPC endpoint service and click **Delete** in the **Operation** column.
6. Click **Yes**.

3.5 Managing Connections of a VPC Endpoint Service

Scenarios


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

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

Prerequisites

There is a VPC endpoint available for connecting to the target 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. 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. Select the **Connection Management** tab.
7. Accept or reject connection of a VPC endpoint in the list based on service requirements.
 - If you click **Accept**, the VPC endpoint can connect to the VPC endpoint service.
 - If you click **Reject**, the VPC endpoint cannot connect to the VPC endpoint service.

3.6 Managing Whitelist Records of a VPC Endpoint Service

Scenarios


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

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

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

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

Add a Whitelist Record


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 domain ID in the required format and click **OK**.

 **NOTE**

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

Delete a Whitelist Record

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, locate the target domain ID, and click **Delete** in the **Operation** column.
To delete multiple whitelist records, select all the target domain IDs and click **Delete** in the upper left corner.
7. Click **Yes**.

3.7 Viewing Port Mappings of a VPC Endpoint Service

Scenarios

After a VPC endpoint service is created, you can view the added port mappings.


A port mapping defines the protocol and ports used for communication between a VPC endpoint and a VPC endpoint service.

- **Protocol:** A protocol both supported by the VPC endpoint and VPC endpoint service
- **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.

 **NOTE**

Port mappings cannot be modified or deleted.

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**.
5. In the VPC endpoint service list, locate the target VPC endpoint service and click its name.
6. On the displayed page, select the **Port Mapping** tab.
The port mapping configured for the VPC endpoint service is displayed.

3.8 Managing Tags of a VPC Endpoint Service

Scenarios

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

A tag is a unique identifier of each VPC endpoint service, and it consists of a tag key and a tag value. You can add a maximum of 10 tags to each VPC endpoint service.

Add a Tag

Perform the following operations to add a tag for an existing 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 **Tags** tab.
7. Click **Add Tag**.
8. In the displayed dialog box, enter a key and a value.
[Table 3-5](#) describes the required parameters.


Table 3-5 Tag requirements for VPC endpoint services

Parameter	Requirement
Tag key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each resource.• Can contain a maximum of 36 Unicode characters.• Cannot start or end with a space or contain special characters =* <> \, /
Tag value	<ul style="list-style-type: none">• Cannot be left blank.• Can contain a maximum of 43 Unicode characters.• Cannot start or end with a space or contain special characters =* <> \, /

9. Click **OK**.

Edit a Tag

Perform the following operations to edit a tag of an existing 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 **Tags** tab.
7. In the tag list, locate the target tag and click **Edit** in the **Operation** column.
8. Enter a new value.

NOTE

You can only edit values of exiting tags.


9. Click **OK**.

Delete a Tag

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

CAUTION

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

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 **Tags** tab.
7. In the tag list, locate the target tag and click **Delete** in the **Operation** column.
8. Click **Yes**.

4 VPC Endpoints

4.1 VPC Endpoint Overview

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

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

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

Table 4-1 Management of VPC endpoints

Operation	Description	Constraint
Creating a VPC Endpoint	Describes how to create a VPC endpoint.	<ul style="list-style-type: none">• VPC endpoints are region-level resources. Select a region and project when you create such an endpoint.• Each tenant can create a maximum of 50 VPC endpoints.• When you create a VPC endpoint, ensure that the associated VPC endpoint service exists and is in the same region as the VPC endpoint.
Querying and Accessing a VPC Endpoint	Describes how to query summary of a VPC endpoint.	A VPC endpoint supports a maximum of 3000 concurrent requests.
Deleting a VPC Endpoint	Describes how to delete a VPC endpoint.	Deleted VPC endpoints cannot be recovered. Exercise caution when performing this operation.

Operation	Description	Constraint
Managing Tags of a VPC Endpoint	Describes how to manage VPC endpoint tags, including viewing, adding, editing, and deleting tags.	A maximum of 10 tags can be added to each VPC endpoint.

4.2 Creating a VPC Endpoint

Scenarios

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

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

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

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

You can create different types of VPC endpoints based the types of associated VPC endpoint services:

- [Creating a VPC Endpoint for Accessing Interface VPC Endpoint Services](#)
- [Creating a VPC Endpoint for Accessing Gateway VPC Endpoint Services](#)

Creating a VPC Endpoint for Accessing Interface VPC Endpoint Services


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 displayed page, click **Create VPC Endpoint**.
5. On the **Create VPC Endpoint** page, configure the parameters.

Table 4-2 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.

Parameter	Description
Service Category	<p>There are two options as follows:</p> <ul style="list-style-type: none"> • Cloud services: Select this value if the target VPC endpoint service is a cloud service. • Find a service by name: Select this value if the target VPC endpoint service is a private service of your own.
Service List	<p>This parameter is available only when you select Cloud services for Service Category.</p> <p>The VPC endpoint service has been created by operations people and you can use it without having to perform the creation operation.</p>
VPC Endpoint Service Name	<p>This parameter is available only when you select Find a service by name for Service Category.</p> <p>In the VPC endpoint service list, locate the target VPC endpoint service, copy its name in the Name column, paste it into the VPC Endpoint Service Name text box, and click Verify.</p> <ul style="list-style-type: none"> • If Service name found is displayed, proceed with subsequent operations. • If Service name not found is displayed, check whether the region is the same as that of the connected VPC endpoint service or whether the entered service name is correct.
Private Domain Name	<p>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.</p> <p>This parameter is only configured for interface VPC endpoints.</p> <ul style="list-style-type: none"> • 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 located.
Subnet	<p>This parameter is available when you want to access an interface endpoint service.</p> <p>Specifies the subnet where the VPC endpoint is located.</p>
Tag	<p>This parameter is optional.</p> <p>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.</p> <p>Tag keys and values must meet requirements listed in Table 4-3.</p>

Table 4-3 Tag requirements for VPC endpoints

Parameter	Requirement
Tag key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each resource.• Can contain a maximum of 36 Unicode characters.• Cannot start or end with a space or contain special characters =*<>\ /
Tag value	<ul style="list-style-type: none">• 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 **Create Now**.
 - 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**.

Creating a VPC Endpoint for Accessing Gateway VPC Endpoint Services


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 displayed page, click **Create VPC Endpoint**.
5. On the **Create VPC Endpoint** page, configure the parameters.

Table 4-4 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.
Service Category	Specifies the type of services that are configured as gateway VPC endpoint services. Only cloud services are supported. Select Cloud services .

Parameter	Description
Service List	<p>This parameter is available only when you select Cloud services for Service Category.</p> <p>In the VPC endpoint service list, select the VPC endpoint service whose type is gateway.</p> <p>The VPC endpoint service has been created by operations people and you can use it without having to perform the creation operation.</p>
VPC	Specifies the VPC where the VPC endpoint is deployed.
Tag	<p>This parameter is optional.</p> <p>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.</p> <p>Tag keys and values must meet requirements listed in Table 4-5.</p>

Table 4-5 Tag requirements for VPC endpoints

Parameter	Requirement
Tag key	<ul style="list-style-type: none"> • Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 36 Unicode characters. • Cannot start or end with a space or contain special characters =* <> \, /
Tag value	<ul style="list-style-type: none"> • 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 **Create Now**.
 - 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**.


4.3 Querying and Accessing a VPC Endpoint

Scenarios


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


Querying a VPC Endpoint

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


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**.

On the displayed page, locate the target VPC endpoint by entering a keyword in the search box in the upper right corner:

- Search by VPC endpoint service name or VPC endpoint ID.
 - i. Select **VPC endpoint service name** or **ID** in the filter box.
 - ii. Enter a keyword in the search box.
 - iii. Click  to start the search.

VPC endpoints containing the keyword are displayed in the VPC endpoint list.
 - Search by preset tag.
 - i. Click  in **Search by Tag**.
 - ii. Enter a tag and a value.

Enter a key or value or select a key or value from the drop-down list.
You can use a maximum of 10 tags to search for a VPC endpoint.
 - iii. Click **Search**.

VPC endpoints containing the specified tag are displayed in the VPC endpoint list.
If you set multiple tags, VPC endpoints containing all the specified tags will be displayed.
4. In the VPC endpoint list, click  before the target VPC endpoint to view its details.

After a VPC endpoint is created, a private IP address is assigned.

Table 4-6 Required parameters

Parameter	Description
VPC Endpoint Service Name	Specifies the name of the VPC endpoint service that the VPC endpoint is used to access.
Private IP Address	Specifies the IP address for accessing the VPC endpoint.
Private Domain Name	Specifies the private domain name for accessing the VPC endpoint.

Accessing a VPC Endpoint Using a Private IP Address

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

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

Command Private IP address:Port number

The following is a command example:

curl *Private IP address:Port number*

Accessing a VPC Endpoint (Using a Private Domain Name)

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

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

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

Viewing the record set of the private domain name

1. Log in to the management console.
2. In the service list, choose **Network > Domain Name Service**.
The DNS console is displayed.
3. In the navigation pane, choose **Private Zones**.
The **Private Zones** page is displayed.
4. In the private zone list, click the name of the target private zone.
The record set page is displayed.
5. In the record set list, locate the target A record set and view its information.
When the value in the **Status** column changes to **Normal**, the resolution takes effect.

Accessing a VPC endpoint using a private domain name

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

Command Private domain name:Port number

The following is a command example:

curl *Private domain name:Port number*

4.4 Deleting a VPC Endpoint


Scenarios

This section describes how to delete a VPC endpoint.

NOTE

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

Procedure

1. 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 Endpoints**.
5. In the VPC endpoint list, locate the target VPC endpoint and click **Delete** in the **Operation** column.
6. Click **Yes**.

4.5 Managing Tags of a VPC Endpoint



Scenarios

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

Each VPC endpoint has a unique tag, which consists of a tag key and a tag value. You can add a maximum of 10 tags to each VPC endpoint.

Add a Tag

Perform the following operations to add a tag for an existing VPC endpoint:

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 VPC endpoint list, locate the target VPC endpoint and click  in front of the endpoint.
5. On the displayed page, select the **Tags** tab.
6. Click **Add Tag**.
7. In the displayed dialog box, enter a key and a value.

[Table 4-7](#) describes the parameter requirements.



Table 4-7 Tag requirements for VPC endpoints

Parameter	Requirement
Tag key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each resource.• Can contain a maximum of 36 Unicode characters.• Cannot start or end with a space or contain special characters =*<>\ /
Tag value	<ul style="list-style-type: none">• Cannot be left blank.• Can contain a maximum of 43 Unicode characters.• Cannot start or end with a space or contain special characters =*<>\ /

8. Click **OK**.

Edit a Tag

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

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 VPC endpoint list, locate the target VPC endpoint and click  in front of the endpoint.
5. On the displayed page, select the **Tags** tab.
6. In the tag list, locate the target tag and click **Edit** in the **Operation** column.
7. Enter a new value.

NOTE

You can only edit the tags that have values.

8. Click **OK**.



Delete a Tag

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

CAUTION

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

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 VPC endpoint list, locate the target VPC endpoint and click  in front of the endpoint.
5. On the displayed page, select the **Tags** tab.
6. In the tag list, locate the target tag and click **Delete** in the **Operation** column.
7. Click **Yes**.

5 Permission Management

5.1 Creating a User and Granting Permissions

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

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to VPCEP resources.
- Grant only the permissions required for users to perform a task.
- Entrust an account or cloud service to perform professional and efficient O&M on your VPCEP resources.

If your account does not require individual IAM users, skip over this section.

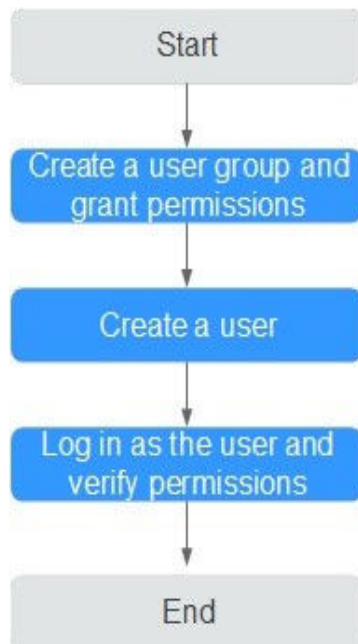
Figure 5-1 shows the procedure for granting permissions.

Prerequisites

Learn about the permissions.

Authorization Process

Figure 5-1 Process for granting VPCEP permissions



1. **Create a user group and assign permissions.**
Create a user group on the IAM console and assign the policy to the group.
2. **Create a user and add the user to the user group.**
Create a user on the IAM console and add the user to the group created in 1.
3. **Log in to the management console as the created user.**
Log in to the VPCEP console by using the newly created user, and verify that the user only has read permissions for VPCEP.
 - Click **Service List** and choose **VPC Endpoint**. On the displayed page, click **Buy VPC Endpoint** in the upper right corner. If you can buy a VPC endpoint, the policy has already taken effect.
 - Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the policy has already taken effect.

6 FAQs



6.1 What Is a Quota?

What Is a Quota?

Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number and capacity of resources available to users, for example, how many cloud resources you can create.

You can also increase the quota if the existing quota cannot meet your service requirements.

How Do I View My Quotas?

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, click  .
The **Service Quota** page is displayed.
4. View the used and total quota of each type of resources on the displayed page.

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

6.2 How Can I Check Network Configurations of the ECS Hosting the VPC Endpoint Service?

1. Confirm that the security group of the ECS NIC is correctly configured.
 - On the ECS details page, view the security group details.
 - Check whether the security group permits IP addresses in the 198.19.128.0/20 network segment in the inbound direction. If it does not, add inbound rules for this network segment based on service requirements.

2. Confirm that the network ACL of the subnet used by the ECS NIC does not block traffic.

If you can configure the network ACL on the left part of the VPC console, confirm that the subnet of the associated VPC endpoint allows traffic to pass through.

6.3 What Are the Differences Between VPC Endpoints and VPC Peering Connections?

Table 6-1 describes differences between VPC endpoints and VPC peering connections.

NOTE

VPC endpoints and VPC peering connections are two different resources. You can configure either of them based on your connectivity needs.

Table 6-1 Differences

Category	VPC Peering Connection	VPC Endpoint
Security	All resources in a VPC, such as ECSs and load balancers, can be accessed.	Allows access to a specific service or application. Only the ECSs and load balancers in the VPC for which VPC endpoint services are created can be accessed.
CIDR block overlap	Not supported If two VPCs have overlapping subnets, the VPC peering connection will not work.	Supported If you use a VPC endpoint to connect two VPCs, you do not have to worry about overlapping subnets.
Communication mode	VPCs connected through a peering connection can communicate with each other.	Requests can only be initiated from a VPC endpoint to a VPC endpoint service, but not the other way around.
Route configuration	If a peering connection is established between two VPCs, you need to add routes to the VPCs so that they can communicate with each other.	For two VPCs that are connected through a VPC endpoint, the route has been configured, and you do not need to configure it again.

Category	VPC Peering Connection	VPC Endpoint
Access using VPN/Direct Connect	Supported You can create a VPC Peering connection to connect your local data center to a cloud service using a VPN connection or a direct connection.	Supported You can create a VPC endpoint to connect your local data center to a cloud service using a VPN connection or a direct connection over an internal network.

6.4 What Are Statuses of VPC Endpoint Services and VPC Endpoints?

Table 6-2 describes statuses of a VPC endpoint service and their meanings.

Table 6-2 Statuses of a VPC endpoint service

Status	Description
Creating	Indicates that the VPC endpoint service is being created.
Available	Indicates that the VPC endpoint service is created and can accept a VPC endpoint.
Failed	Indicates that the VPC endpoint service fails to be created.
Deleting	Indicates that the VPC endpoint service is being deleted.
Deleted	Indicates that the VPC endpoint service has been deleted.

Table 6-3 describes statuses of a VPC endpoint and their meanings.

Table 6-3 Statuses of a VPC endpoint

Status	Description
Pending acceptance	Indicates that the VPC endpoint is pending acceptance of the owner of the associated VPC endpoint service.
Creating	Indicates that the VPC endpoint is connecting to the associated VPC endpoint service.
Accepted	Indicates that the VPC endpoint is accepted by the associated VPC endpoint service.
Rejected	Indicates that the VPC endpoint is rejected by the associated VPC endpoint service.

Status	Description
Failed	Indicates that the VPC endpoint fails to connect to the associated VPC endpoint service.
Deleting	Indicates that the VPC endpoint is being deleted.

A Change History

Released On	Description
2020-07-31	This issue is the first official release.

Released On	Description
2020-11-06	This issue is the first official release.