VPC Endpoint

User Guide

Issue	01
Date	2020-12-11

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Service Overview

1.1 What Is VPC Endpoint?

VPC Endpoint 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 VPC Endpoint. 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 VPC Endpoint works

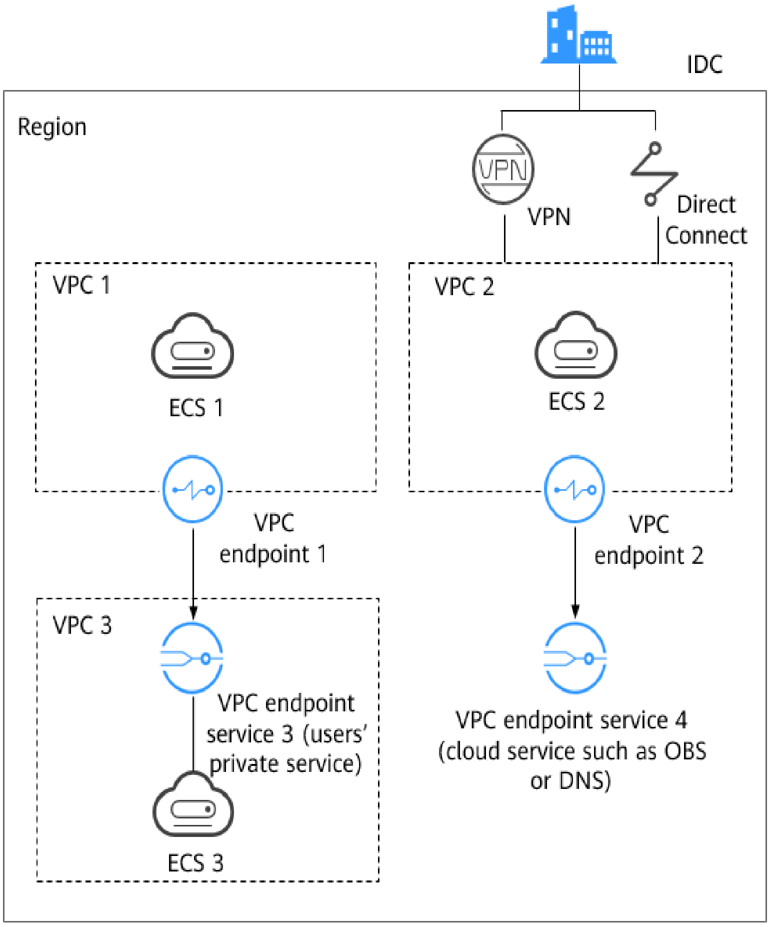

IDC
Region
VPN
Direct Connect
VPC 1
ECS 1
VPC endpoint 1
VPC 2
ECS 2
VPC endpoint 2
VPC 3
VPC endpoint service 3 (users' private service)
ECS 3
VPC endpoint service 4 (cloud service such as OBS or DNS)

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 VPC Endpoint

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

- Web-based console

  You can access VPC Endpoint using the web-based console.

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

- APIs

Use this method if you need to integrate VPC Endpoint into 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

VPC Endpoint 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 VPC Endpoint 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

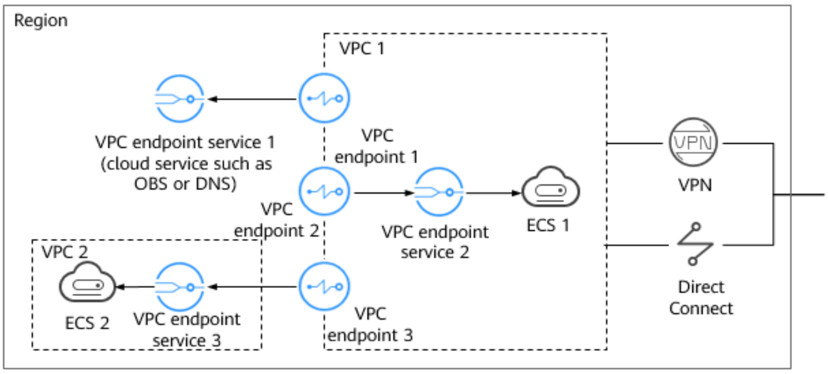


Figure 1-2 shows the process of connecting an IDC to VPC 1 over VPN or Direct Connect, for the purposes of:

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

For cloud migration, VPC Endpoint 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 VPC Endpoint, 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 the Private IP Address of OBS over Private Networks**.

Cross-VPC Connection

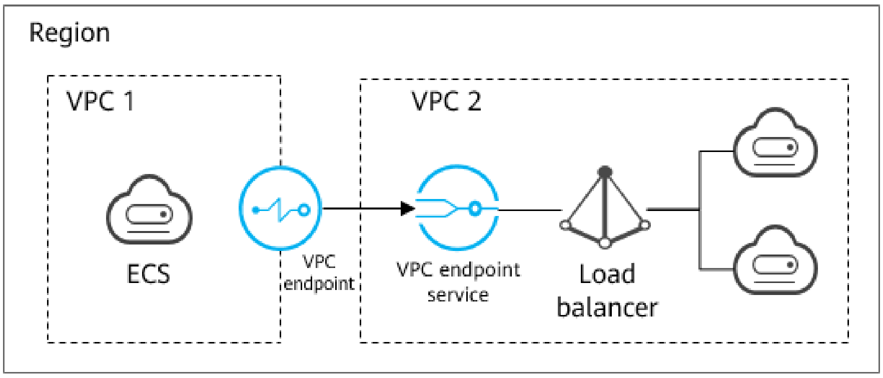
With VPC Endpoint, resources in two different VPCs can communicate with each other despite of logic isolation between them as long as the two VPCs are in the same region.

NOTE

VPC endpoints and VPC peering connections are different in security, communications 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.

VPC Endpoint has the following advantages:

- High performance

  Each gateway supports up to one million concurrent connections.

- Simplified operations

  VPC Endpoint resources can be created within seconds and take effect quickly.

For details, see the following sections:

- **Configuring a VPC Endpoint for Communications Across VPCs of the Same Domain**
- **Configuring a VPC Endpoint for Communications Across VPCs of Different Domains**

1.4 Constraints

Resource Quotas

Table 1-1 describes constraints on the VPC Endpoint resource quota.

Table 1-1 VPC Endpoint resource quotas

Resource	Default Quota	How to Increase Quota
VPC endpoint services per account in one region	20	**Quotas**
VPC endpoints per account in one region	50	**Quotas**

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 connect to only one VPC endpoint service.
- A VPC endpoint supports a maximum of 3,000 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 VPC Endpoint and Other Services

Table 1-2 shows the relationship between VPC Endpoint 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	• **Configuring a VPC Endpoint for Communications Across VPCs of the Same Domain** • **Configuring a VPC Endpoint for Communications 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 VPC Endpoint	VPN	**Configuring a VPC Endpoint for Accessing the Private IP Address of OBS over Private Networks**
Connecting an IDC to your VPC using a Direct Connect connection and connecting your VPC to a cloud service through VPC Endpoint	Direct Connect	**Configuring a VPC Endpoint for Accessing the Private IP Address of OBS over Private Networks**
When an enterprise needs to provide VPC Endpoint for multiple users, IAM can be used to create users and control access of these domains to enterprise resources.	IAM	N/A
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.	ELB	**Creating a VPC Endpoint Service**
Configuring a private service as a VPC endpoint service. You can create a VPC endpoint to access the VPC endpoint service.	ECS	**Creating a VPC Endpoint Service**

Interactive Function	Service	Reference
Configuring a private service as a VPC endpoint service. You can create a VPC endpoint to access the VPC endpoint service.	BMS	**Creating a VPC Endpoint Service**

1.6 Permissions

If you need to assign different permissions to employees in your enterprise to access your VPC Endpoint resources, you can use Identity and Access Management (IAM) to manage fine-grained permissions. IAM provides identity authentication, permissions management, and access control, helping you to securely access your cloud resources.

With IAM, you can use your account to create IAM users and assign permissions to control their access to specific cloud resources. For example, if you want website maintenance personnel in your enterprise to use VPC Endpoint resources but do not want them to delete other cloud resources or perform any other high-risk operations, you can create IAM users and grant only permissions to use VPC Endpoint resources.

If your account does not require individual IAM users for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account.

For more information about IAM, see **IAM Service Overview**.

VPC Endpoint Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

VPC Endpoint is a project-level service deployed for specific regions. You need to select a project for which the permissions will be granted. If you select **All projects**, the permissions will be granted for all the projects. When accessing VPC Endpoint, the users need to switch to the authorized region.

Table 1-3 lists all system-defined roles for VPC Endpoint.

Table 1-3 System-defined for VPC Endpoint

Role	Description	Type	Dependency
VPCEndpoint Administrator	Full permissions for VPC Endpoint	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 supported by system-defined permissions for VPC Endpoint.

Table 1-4 Common operations supported by system-defined permissions

Operation	VPCEndpoint Administrator
Creating a VPC endpoint	√
Deleting a VPC endpoint	√
Querying a VPC endpoint	√
Modifying a VPC endpoint	√
Creating a VPC endpoint service	√
Deleting a VPC endpoint service	√
Querying a VPC endpoint service	√
Modifying a VPC endpoint service	√

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

NOTE

Supported cloud services vary in different regions. For details, see the 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	EU-Paris: ● com.orange-business.prod-cloud-ocb.eu-west-0.obs ● com.orange-business.cloud-ocb.eu-west-0.obs-internet	If you want to access OBS: ● Using its private address, select the endpoint service ending with **obs**. ● Using its public address, select the endpoint service ending with **obs-internet**.

Interface VPC Endpoint Services

Interface VPC endpoint services are mainly configured from:

- Cloud services. You do not have the permissions to configure such VPC endpoint services but can select them when creating a VPC endpoint.
- Your private services

NOTE

Supported cloud services vary in different regions. For details, see the 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	EU-Paris: com.orange-business.prod-cloud-ocb.eu-west-0.dns	Select the endpoint service ending with **dns** if you want to access DNS over private networks.
API Gateway	Cloud service	Interface	EU-Paris: com.orange-business.prod-cloud-ocb.eu-west-0.api	Select the endpoint service ending with **api** if you want to access API Gateway using a VPC endpoint.
ELB	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.
BMS	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.

VPC Endpoint 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

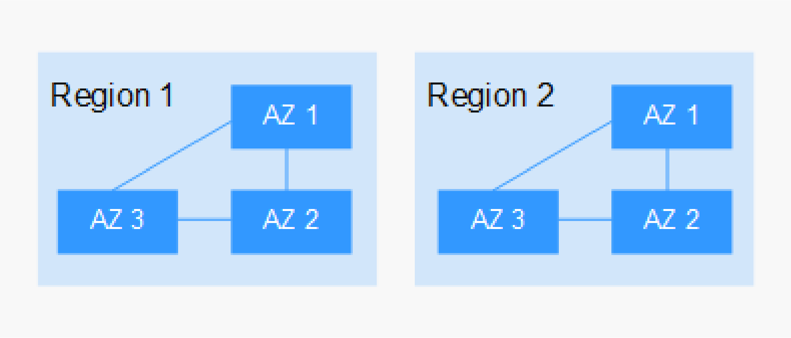
Concept

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 VPC Endpoint.

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

Application Scenarios

VPC Endpoint can be used in different scenarios. For details, see **Table 2-1**.

Table 2-1 Application scenarios

Scenario	Description
Communications 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: ● **Configuring a VPC Endpoint for Communications Across VPCs of the Same Domain** ● **Configuring a VPC Endpoint for Communications Across VPCs of Different Domains**
Access to cloud resources from an on-premises data center	VPC Endpoint allows you to access cloud resources from your on-premises data center. For details, see the following sections: ● **Configuring a VPC Endpoint for Accessing the Private IP Address of OBS over Private Networks** ● **Configuring a VPC Endpoint for Accessing the Public IP Address of OBS over Public Networks**

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

2.2.1 Overview

Scenarios

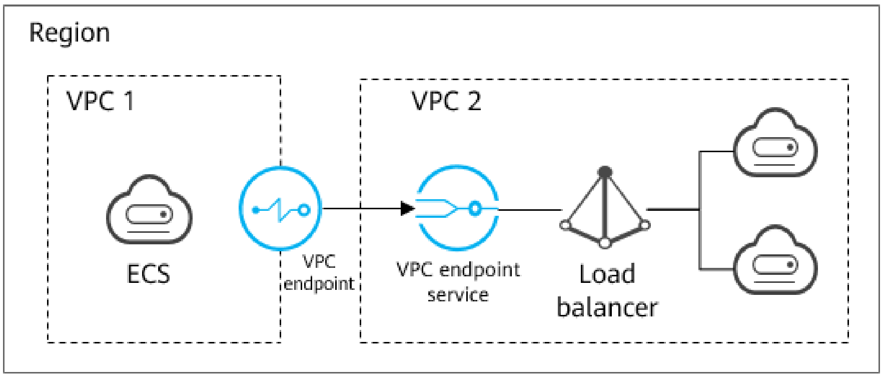
With VPC Endpoint, you can access resources across VPCs in the same region.

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

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

VPC 1 and VPC 2 belong to the same domain in the same region. You can configure ELB in VPC 2 as a VPC endpoint service and create a VPC endpoint in VPC 1. Then the ECS in VPC 1 can access ELB in VPC 2 using the private IP address.

Figure 2-1 Cross-VPC communications



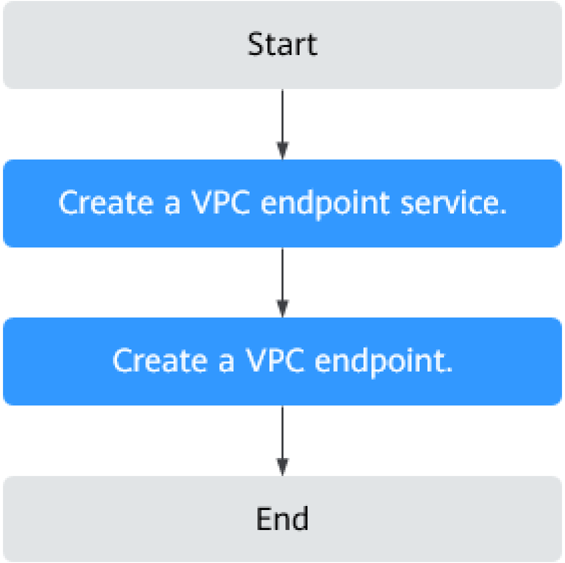
NOTE

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

Configuration Process

Figure 2-2 shows how to enable communications between VPCs of the same domain using VPC Endpoint.

Figure 2-2 Cross-VPC communications



2.2.2 Step 1: Create a VPC Endpoint Service

Scenarios

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

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

Prerequisites

There is a load balancer in the VPC where you are going to create the VPC endpoint service.

Procedure

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

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

5. Configure required parameters.

Table 2-2 Parameters for creating a VPC endpoint service

Parameter	Description
Region	Specifies the region where the VPC endpoint service is to be deployed. Resources in different regions cannot communicate with each other over an intranet. For lower latency and quicker access, select the nearest region.
Name	This parameter is optional. Specifies the name of the VPC endpoint service. The name can contain a maximum of 16 characters, including letters, digits, underscores (_), and hyphens (-). ● If you do not enter a name, the system generates a name in **{region}.{service_id}** format. ● If you enter a name, the system generates a name in **{region}.{Name}.{service_id}** format.
VPC	Specifies the VPC where the VPC endpoint service is to be deployed.
Service Type	Specifies the type of the VPC endpoint service. The type can only be **Interface**.
Connection Approval	Specifies whether the connection between a VPC endpoint and a VPC endpoint service requires approval from the owner of the VPC endpoint service. You can enable or disable **Connection Approval**. When **Connection Approval** is enabled, any VPC endpoint for connecting to the VPC endpoint service needs to be approved. For details, see step **7**.
Port Mapping	Specifies the protocol and ports used for communications between the VPC endpoint service and a VPC endpoint. The protocol is TCP. ● **Service Port**: provided by the backend resource bound to the VPC endpoint service. ● **Terminal Port**: provided by the VPC endpoint, allowing you to access the VPC endpoint service. The service and terminal port numbers range from **1** to **65535**. A maximum of 50 port mappings can be added at a time. **NOTE** Accessing a VPC endpoint service from a VPC endpoint is to access the service port from the associated terminal port.

Parameter	Description
Backend Resource Type	Specifies the backend resource that provides services to be accessed. The following backend resource types are supported: ● **Elastic load balancer**: Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance. ● **ECS**: Backend resources of this type serve as servers. ● **BMS**: Backend resources of this type serve as servers. In this example, select **Elastic load balancer**. **NOTE** ● For the security group associated with the backend resource configured for the VPC endpoint service, add an inbound rule, with **Source** set to **198.19.128.0/17**. For details, see section "Adding a Security Group Rule" in the *Virtual Private Cloud User Guide*. ● If you configure a load balancer as the backend resource for the VPC endpoint service, and enable access control for the listener associated with the load balancer, ensure to allow traffic from 198.19.128.0/17.
Load Balancer	When **Backend Resource Type** is set to **Elastic load balancer**, select the load balancer that provides services from the drop-down list. **NOTE** If an elastic load balancer is used as the backend resource, the source IP address received by the VPC endpoint service is not the real address of the client.
Tag	This parameter is optional. Specifies the VPC endpoint service tag, which consists of a key and a value. You can add up to 10 tags to each VPC endpoint service. Tag keys and values must meet requirements listed in **Table 2-3**.

Table 2-3 Tag requirements for VPC endpoint services

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

Parameter	Requirement
Tag value	● Cannot be left blank. ● Can contain a maximum of 43 characters. ● Cannot start or end with a space or contain special characters =*<>\,|/

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

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.

NOTE

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

Procedure

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

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

Table 2-4 VPC endpoint parameters

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

Parameter	Description
Service Category	There are two options: ● **Cloud services**: Select this value if the target VPC endpoint service is a cloud service. ● **Find a service by name**: Select this value if the target VPC endpoint service is a private service of your own. In this example, select **Find a service by name**.
VPC Endpoint Service Name	This parameter is available only when you select **Find a service by name** for **Service Category**. Enter the VPC endpoint service name recorded in step 8, and click **Verify**. ● If "Service name found." is displayed, proceed with subsequent operations. ● If "Service name not found." is displayed, check whether the region is the same as that of the VPC endpoint service or whether the name entered is correct.
Create a Private Domain Name	If you want to access a VPC endpoint using a domain name, select **Create a Private Domain Name**. This parameter is mandatory when the VPC endpoint will be used to access an interface VPC endpoint service.
VPC	Specifies the VPC where the VPC endpoint is to be deployed.
Subnet	Specifies the subnet where the VPC endpoint is to be located.
Private IP Address	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. Specifies the private IP address of the VPC endpoint. You can select **Automatically assign** or **Manually specify**.
Access Control	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. It controls IP addresses and CIDR blocks that are allowed to access the VPC endpoint. ● If **Access Control** is enabled, only IP addresses or CIDR blocks in the whitelist are allowed to access the VPC endpoint. ● If **Access Control** is disabled, any IP address or CIDR block can access the VPC endpoint.

Parameter	Description
Whitelist	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. Lists the IP addresses or CIDR blocks that are allowed to access the VPC endpoint. You can add a maximum of 20 records.
Tag	This parameter is optional. Specifies the VPC endpoint tag, which consists of a key and a value. You can add up to 10 tags to each VPC endpoint. Tag keys and values must meet requirements listed in **Table 2-5**.

Table 2-5 Tag requirements for VPC endpoints

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

6. Confirm the specifications and click **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 VPC endpoint service, ask the owner of the VPC endpoint service to perform the following operations:

   a. In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoint Services**.
   b. Locate the target VPC endpoint service and click its name.
   c. On the displayed page, select the **Connection Management** tab.

- If you allow a VPC endpoint to connect to this VPC endpoint service, locate the target VPC endpoint and click **Accept** in the **Operation** column.
- If you do not allow a VPC endpoint to connect to this VPC endpoint service, click **Reject** in the **Operation** column.

d. Go back to the VPC endpoint list and check whether the status of the target VPC endpoint changes to **Accepted**. If yes, the VPC endpoint is connected to the VPC endpoint service.

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

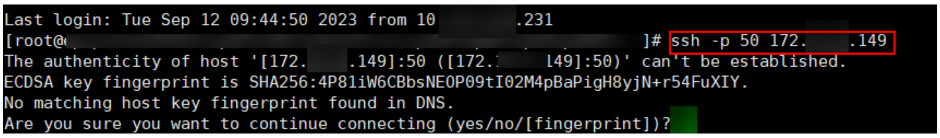
   After a VPC endpoint is created, a private IP address is assigned together with a private domain name if you select **Create a Private Domain Name** during creation.

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

Configuration Verification

Remotely log in to an ECS in VPC 1 and access the private IP address or private domain name of the VPC endpoint.

Figure 2-3 Logging in to an ECS to access the VPC endpoint



```
Last login: Tue Sep 12 09:44:50 2023 from 10[redacted].231
[root@[redacted]]# ssh -p 50 172.[redacted].149
The authenticity of host '[172.[redacted].149]:50 ([172.[redacted]149]:50)' can't be established.
ECDSA key fingerprint is SHA256:4P81iW6CBbsNEOP09tI02M4pBaPigH8yjN+r54FuXIY.
No matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

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

2.3.1 Overview

Scenarios

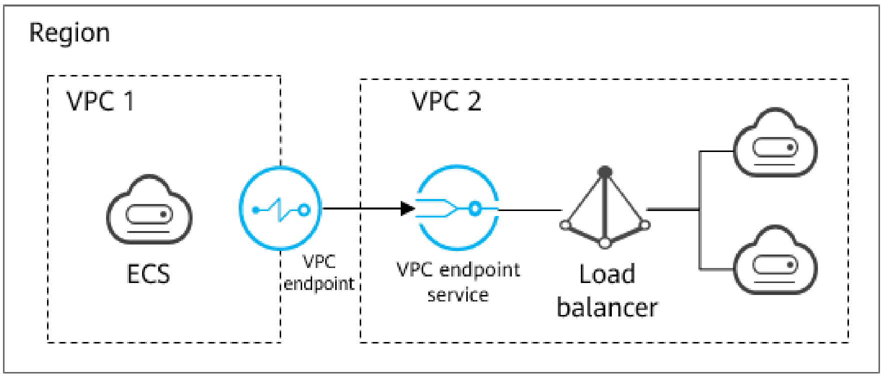
With VPC Endpoint, you can access resources across VPCs in the same region.

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

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

VPC 1 and VPC 2 belong to different domains. You can configure ELB in VPC 2 as a VPC endpoint service and create a VPC endpoint in VPC 1 so that the ECS in VPC 1 can access ELB in VPC 2 using a private IP address.

Figure 2-4 Cross-VPC communications



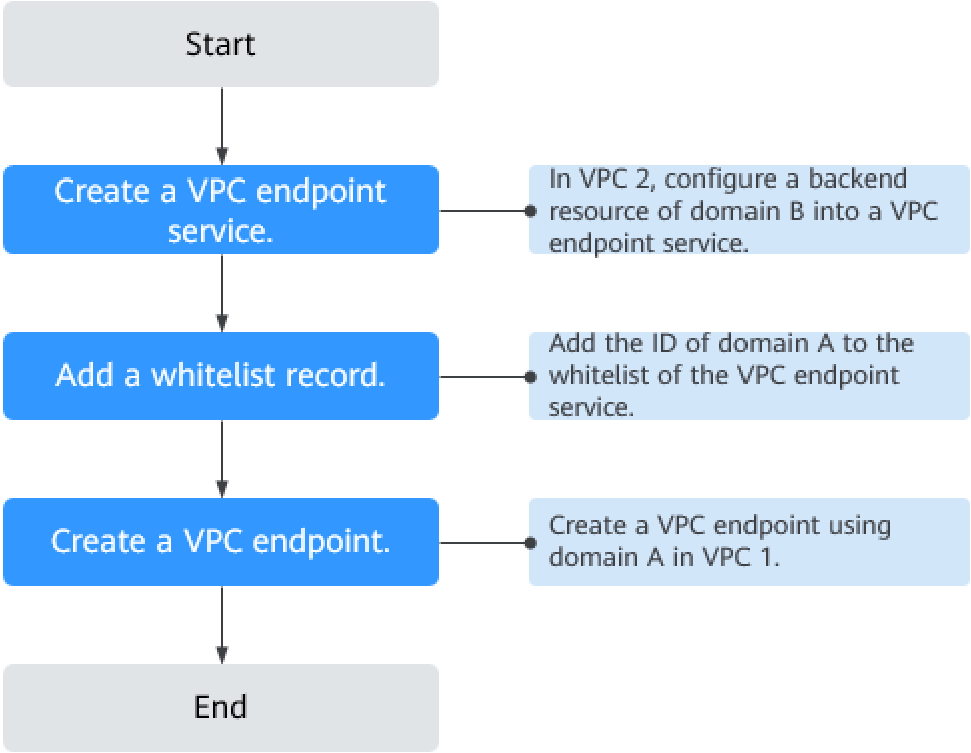
NOTE

- Only one-way communications from the VPC endpoint to the VPC endpoint service are 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 communications between two VPCs of the same domain, see **Configuring a VPC Endpoint for Communications Across VPCs of the Same Domain**.

Cross-VPC Communications

Figure 2-5 shows how to enable communications between two VPCs of different domains using VPC Endpoint.

Figure 2-5 Cross-VPC communications flowchart


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

2.3.2 Step 1: Create a VPC Endpoint Service

Scenarios

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

This section 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 is a load balancer in the VPC where you are going to create the VPC endpoint service.

Procedure

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

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

5. Configure required parameters.

Table 2-6 Parameters for creating a VPC endpoint service

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

Parameter	Description
Connection Approval	Specifies whether the connection between a VPC endpoint and a VPC endpoint service requires approval from the owner of the VPC endpoint service. You can enable or disable **Connection Approval**. When **Connection Approval** is enabled, any VPC endpoint for connecting to the VPC endpoint service needs to be approved. For details, see step 7.
Port Mapping	Specifies the protocol and ports used for communications between the VPC endpoint service and a VPC endpoint. The protocol is TCP. ● **Service Port**: provided by the backend resource bound to the VPC endpoint service. ● **Terminal Port**: provided by the VPC endpoint, allowing you to access the VPC endpoint service. The service and terminal port numbers range from **1** to **65535**. A maximum of 50 port mappings can be added at a time. **NOTE** Accessing a VPC endpoint service from a VPC endpoint is to access the service port from the associated terminal port.
Backend Resource Type	Specifies the backend resource that provides services to be accessed. The following backend resource types are supported: ● **Elastic load balancer**: Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance. ● **ECS**: Backend resources of this type serve as servers. ● **BMS**: Backend resources of this type serve as servers. In this example, select **Elastic load balancer**. **NOTE** ● For the security group associated with the backend resource configured for the VPC endpoint service, add an inbound rule, with **Source** set to **198.19.128.0/17**. For details, see section "Adding a Security Group Rule" in the *Virtual Private Cloud User Guide*. ● If you configure a load balancer as the backend resource for the VPC endpoint service, and enable access control for the listener associated with the load balancer, ensure to allow traffic from 198.19.128.0/17.
Load Balancer	When **Backend Resource Type** is set to **Elastic load balancer**, select the load balancer that provides services from the drop-down list. **NOTE** If an elastic load balancer is used as the backend resource, the source IP address received by the VPC endpoint service is not the real address of the client.

Parameter	Description
Tag	This parameter is optional. Specifies the VPC endpoint service tag, which consists of a key and a value. You can add up to 10 tags to each VPC endpoint service. Tag keys and values must meet requirements listed in **Table 2-7**.

Table 2-7 Tag requirements for VPC endpoint services

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

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

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 or delete an authorized domain ID to and from the whitelist of the VPC endpoint service.

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

Prerequisites

The required VPC endpoint service is available.

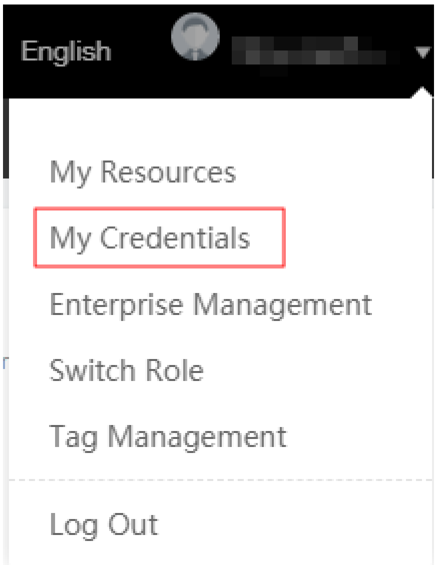
Constraints

- The VPC endpoint and the VPC endpoint service must be deployed in the same region.
- Before you configure the whitelist for a VPC endpoint service, obtain the domain ID of the associated VPC endpoint.

Obtain the ID of Your Own Domain

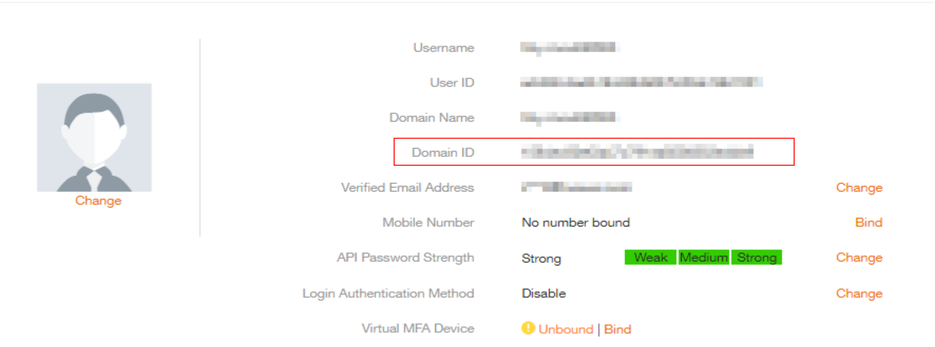
1. Log in to the management console.
2. Click **My Credentials** under the domain.

Figure 2-6 My Credentials



The **My Credentials** page is displayed. You can view the domain ID.

Figure 2-7 My Credentials



Username	[redacted]		
User ID	[redacted]		
Domain Name	[redacted]		
Domain ID	[redacted]		
Verified Email Address	[redacted]		Change
Mobile Number	No number bound		Bind
API Password Strength	Strong	Weak Medium Strong	Change
Login Authentication Method	Disable		Change
Virtual MFA Device	Unbound | Bind		

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

1. Click 📍 in the upper left corner and select the required region and project.

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

   NOTE

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

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

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

Table 2-8 VPC endpoint parameters

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

Parameter	Description
Service Category	There are two options: - **Cloud services**: Select this value if the target VPC endpoint service is a cloud service. - **Find a service by name**: Select this value if the target VPC endpoint service is a private service of your own. In this example, select **Find a service by name**.
VPC Endpoint Service Name	This parameter is available only when you select **Find a service by name** for **Service Category**. Enter the VPC endpoint service name recorded in step 8, and click **Verify**. - If "Service name found." is displayed, proceed with subsequent operations. - If "Service name not found." is displayed, check whether the region is the same as that of the VPC endpoint service or whether the name entered is correct.
Create a Private Domain Name	If you want to access a VPC endpoint using a domain name, select **Create a Private Domain Name**. This parameter is mandatory when the VPC endpoint will be used to access an interface VPC endpoint service.
VPC	Specifies the VPC where the VPC endpoint is to be deployed.
Subnet	Specifies the subnet where the VPC endpoint is to be located.
Private IP Address	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. Specifies the private IP address of the VPC endpoint. You can select **Automatically assign** or **Manually specify**.
Access Control	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. It controls IP addresses and CIDR blocks that are allowed to access the VPC endpoint. - If **Access Control** is enabled, only IP addresses or CIDR blocks in the whitelist are allowed to access the VPC endpoint. - If **Access Control** is disabled, any IP address or CIDR block can access the VPC endpoint.

Parameter	Description
Whitelist	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. Lists the IP addresses or CIDR blocks that are allowed to access the VPC endpoint. You can add a maximum of 20 records.
Tag	This parameter is optional. Specifies the VPC endpoint tag, which consists of a key and a value. You can add up to 10 tags to each VPC endpoint. Tag keys and values must meet requirements listed in **Table 2-9**.

Table 2-9 Tag requirements for VPC endpoints

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

6. Confirm the specifications and click **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 VPC endpoint service, ask the owner of the VPC endpoint service to perform the following operations:

   a. In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoint Services**.
   b. Locate the target VPC endpoint service and click its name.
   c. On the displayed page, select the **Connection Management** tab.

- If you allow a VPC endpoint to connect to this VPC endpoint service, locate the target VPC endpoint and click **Accept** in the **Operation** column.
- If you do not allow a VPC endpoint to connect to this VPC endpoint service, click **Reject** in the **Operation** column.

d. Go back to the VPC endpoint list and check whether the status of the target VPC endpoint changes to **Accepted**. If yes, the VPC endpoint is connected to the VPC endpoint service.

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

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

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

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

2.4.1 Overview

Scenarios

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

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

Figure 2-8 Accessing OBS (private address) from an on-premises data center

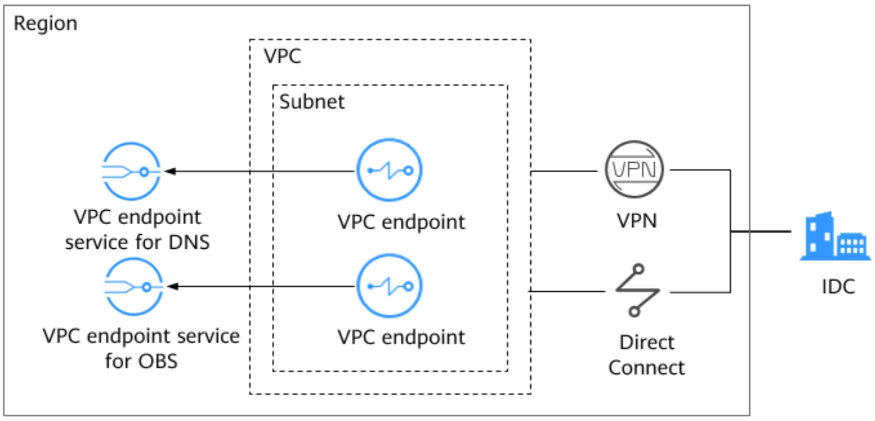


Figure 2-8 shows the process of connecting the on-premise data center to a VPC over VPN or Direct Connect, and then using two VPC endpoints to access DNS and OBS, respectively.

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

The following VPC endpoint services are required:

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

  eu-west-0: **com.orange-business.prod-cloud-ocb.eu-west-0.dns**

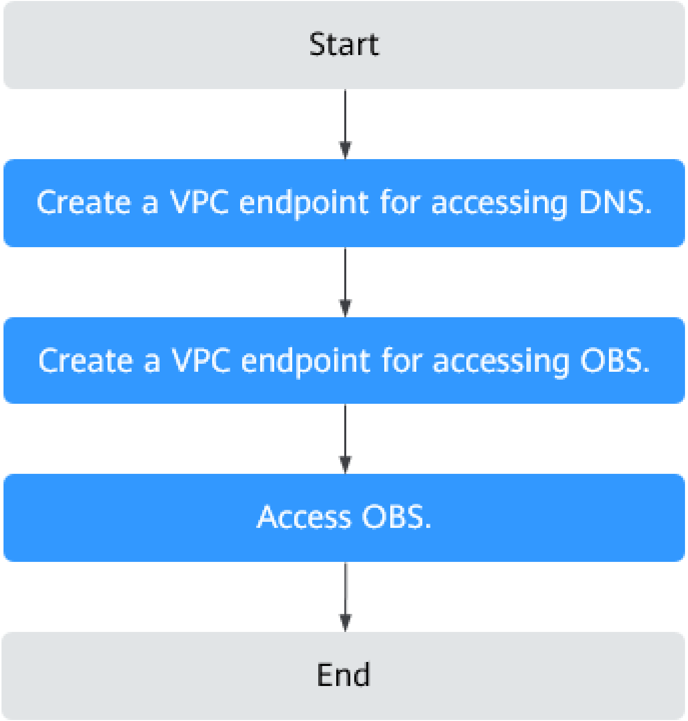
- VPC endpoint service for OBS: provides the OBS service for the on-premises data center.

  eu-west-0: **com.orange-business.prod-cloud-ocb.eu-west-0.obs**

Configuration Process

Figure 2-9 shows the process for configuring a VPC endpoint to access OBS (private address) from the on-premises data center.

Figure 2-9 Configuration flowchart


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

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 is available.

Procedure

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

   The **Create VPC Endpoint** page is displayed.
5. Configure VPC endpoint parameters.

Table 2-10 VPC endpoint parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint is to be located. Resources in different regions cannot communicate with each other over an intranet. For lower latency and quicker access, select the nearest region.
Service Category	There are two options: ● **Cloud services**: Select this value if the target VPC endpoint service is a cloud service. ● **Find a service by name**: Select this value if the target VPC endpoint service is a private service of your own. In this example, select **Cloud services**.
Service List	This parameter is available only when you select **Cloud services** for **Service Category**. The VPC endpoint service has been created by the O&M personnel and you can directly use it. In this example, select **com.orange-business.cloud-ocb.eu-west-0.dns**.
Create a Private Domain Name	If you want to access a VPC endpoint using a domain name, select **Create a Private Domain Name**. This parameter is mandatory when the VPC endpoint will be used to access an interface VPC endpoint service.

Parameter	Description
VPC	Specifies the VPC where the VPC endpoint is to be deployed.
Subnet	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. Specifies the subnet where the VPC endpoint is to be deployed.
Private IP Address	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. Specifies the private IP address of the VPC endpoint. You can select **Automatically assign** or **Manually specify**.
Access Control	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. It controls IP addresses and CIDR blocks that are allowed to access the VPC endpoint. ● If **Access Control** is enabled, only IP addresses or CIDR blocks in the whitelist are allowed to access the VPC endpoint. ● If **Access Control** is disabled, any IP address or CIDR block can access the VPC endpoint.
Whitelist	This parameter is available only when you create a VPC endpoint for connecting to an interface VPC endpoint service. Lists the IP addresses or CIDR blocks that are allowed to access the VPC endpoint. You can add a maximum of 20 records.
Tag	This parameter is optional. Specifies the VPC endpoint tag, which consists of a key and a value. You can add up to 10 tags to each VPC endpoint. Tag keys and values must meet requirements listed in **Table 2-11**.

Table 2-11 Tag requirements for VPC endpoints

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

6. Confirm the specifications and click **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 **com.orange-business.cloud-ocb.eu-west-0.dns** is created.
8. In the VPC endpoint list, click the ID of the target VPC endpoint to view its details.

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

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 on-premises data center.

Prerequisites

The required VPC endpoint service is available.

Procedure

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

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

5. Configure VPC endpoint parameters.

Table 2-12 VPC endpoint parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint is to be located. Resources in different regions cannot communicate with each other over an intranet. For lower latency and quicker access, select the nearest region.
Service Category	There are two options: ● **Cloud services**: Select this value if the target VPC endpoint service is a cloud service. ● **Find a service by name**: Select this value if the target VPC endpoint service is a private service of your own. In this example, select **Cloud services**.
Service List	This parameter is available only when you select **Cloud services** for **Service Category**. The VPC endpoint service has been created by the O&M personnel and you can directly use it. Example: **com.orange-business.cloud-ocb.eu-west-0.obs**
VPC	Specifies the VPC where the VPC endpoint is to be deployed.
Route Table	This parameter is available only when you create a VPC endpoint for connecting to a gateway VPC endpoint service. **NOTE** This parameter is available only in the regions where the route table function is enabled. You are advised to select all route tables. Otherwise, the access to OBS may fail. Select a route table required for the VPC where the VPC endpoint is to be located. For details about how to add routes, see the *Virtual Private Cloud User Guide*.
Tag	This parameter is optional. Specifies the VPC endpoint tag, which consists of a key and a value. You can add up to 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	● Cannot be left blank. ● Must be unique for each resource. ● Can contain a maximum of 36 characters. ● Cannot start or end with a space or contain special characters =*<>\,|/
Tag value	● Cannot be left blank. ● Can contain a maximum of 43 characters. ● Cannot start or end with a space or contain special characters =*<>\,|/

6. Confirm the specifications and click **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 is created.
8. In the VPC endpoint list, click the ID of 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 or Direct Connect connection.

Prerequisites

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

- The VPC subnet that needs to communicate with the on-premises data center over the VPN gateway must include the OBS CIDR block. For details about how to obtain the OBS CIDR block, contact the OBS customer manager.

  For details about how to create a VPN connection, see the *Virtual Private Network User Guide*.
- The VPC subnet that needs to communicate with the on-premises data center over the Direct Connect gateway must include the OBS CIDR block. For details about how to obtain the OBS CIDR block, contact the OBS customer manager.

  For details about how to create a Direct Connect connection, see the *Direct Connect User Guide*.

Procedure

1. In the VPC endpoint list, locate the target VPC endpoint and click the ID of the endpoint to view its details.
2. Add DNS records on the DNS server at your on-premises data center to forward requests for resolving OBS domain names to the VPC endpoint for accessing DNS.

   The methods of configuring DNS forwarding rules vary depending on OSs. For details, see the DNS software operation guides.

   This step uses Bind, a common DNS software, as an example to configure forwarding rules in the UNIX.

   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 on-premises data center, add the private IP address of the VPC endpoint in file **/etc/resolv.conf**.
   - *xx.xx.xx.xx* is the VPC endpoint IP address obtained in **1**.

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

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

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

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

   NOTE

   - *xx.xx.xx.xx* is the VPC endpoint IP address obtained in **1**.
   - *xxx.xxx.xxx.xxx* indicates the IP address of the Direct Connect or VPN gateway created at your on-premises data center.
   - The route command format varies depending on the OS. Use the route command format corresponding to the actual OS.

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

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

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

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

NOTE

- *xxx.xxx.xxx.xxx* indicates the IP address of the Direct Connect or VPN gateway created at your on-premises data center.
- The route command format varies depending on the OS. Use the route command format corresponding to the actual OS.

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

```
telnet bucket.endpoint
```

In the command:

– *bucket*: indicates the bucket name.

– *endpoint*: indicates the OBS endpoint.

Example: **telnet bucket.obs.cn-east-3.myhuaweicloud.com**

NOTE

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

2.5 Configuring a VPC Endpoint for Accessing the Public IP Address of OBS over Public Networks

2.5.1 Overview

Scenarios

If you want to access OBS using its public address from an IDC, you can use a VPC endpoint to connect to the VPC endpoint service configured for OBS.

This section describes how to create such a VPC endpoint to access OBS.

Figure 2-10 Accessing OBS using its public address from an IDC

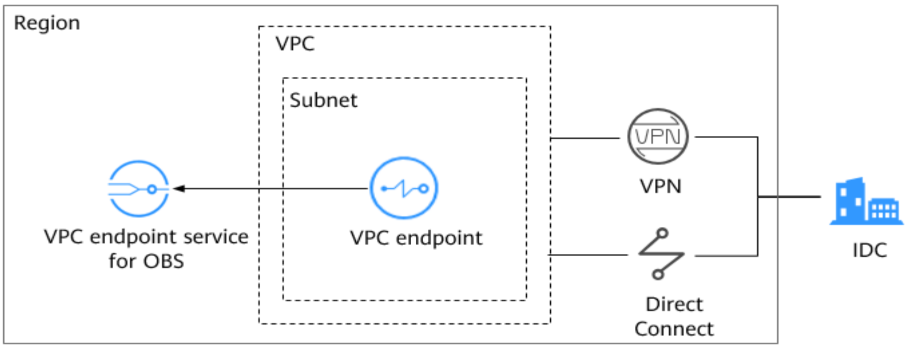


Figure 2-10 shows the process of connecting an IDC to a VPC over VPN or Direct Connect to access OBS using a VPC endpoint created in the VPC.

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

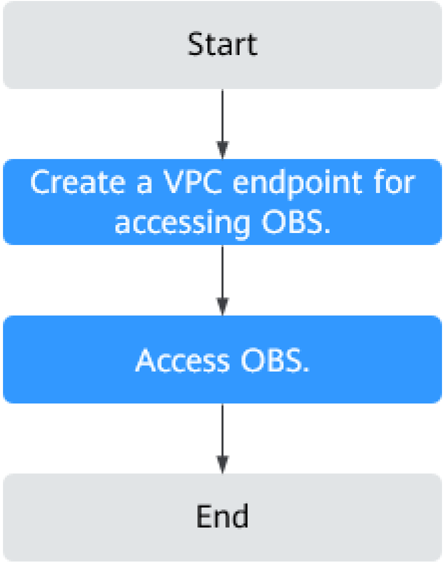
The following VPC endpoint services are required:

eu-west-0: **com.orange-business.prod-cloud-ocb.eu-west-0.obs-internet**

Configuration Process

Figure 2-11 shows the process for configuring a VPC endpoint to access OBS using its public address from an IDC.

Figure 2-11 Configuration flowchart



2.5.2 Step 1: Create a VPC Endpoint for Accessing OBS

Scenarios

This section describes how to create a VPC endpoint to access OBS from an on-premises data center.

Prerequisites

The required VPC endpoint service is available.

Procedure

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

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

5. Configure required parameters.

Table 2-14 VPC endpoint parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint is to be located. Resources in different regions cannot communicate with each other over an intranet. For lower latency and quicker access, select the nearest region.
Service Category	There are two options: ● **Cloud services**: Select this value if the target VPC endpoint service is a cloud service. ● **Find a service by name**: Select this value if the target VPC endpoint service is a private service of your own. In this example, select **Cloud services**.
Service List	This parameter is available only when you select **Cloud services** for **Service Category**. The VPC endpoint service has been created by the O&M personnel and you can directly use it. Select **com.orange-business.prod-cloud-ocb.eu-west-0.obs-internet**.
VPC	Specifies the VPC where the VPC endpoint is to be deployed.
Route Table	This parameter is available only when you create a VPC endpoint for connecting to a gateway VPC endpoint service. **NOTE** This parameter is available only in the regions where the route table function is enabled. You are advised to select all route tables. Otherwise, the access to OBS may fail. Select a route table required for the VPC where the VPC endpoint is to be located. For details about how to add routes, see the *Virtual Private Cloud User Guide*.
Tag	(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 2-15**.

Table 2-15 Tag requirements for VPC endpoints

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

6. Confirm the specifications and click **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 **com.orange-business.prod-cloud-ocb.eu-west-0.obs-internet** is created.
8. In the VPC endpoint list, click the ID of the target VPC endpoint to view its details.

2.5.3 Step 2: Access OBS

Scenarios

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

Prerequisites

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

- The VPC subnet associated with the VPN gateway contains the OBS CIDR block.

  For details about how to create a VPN connection, see the *Virtual Private Network User Guide*.
- The VPC subnet associated with the Direct Connect gateway contains the OBS CIDR block.

  For details about how to create a Direct Connect connection, see the *Direct Connect User Guide*.

Procedure

Configure an OBS route from the on-premises data center to the VPN or Direct Connect gateway.

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

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

```
route -p add Public IP address xxx.xxx.xxx.xxx
```

NOTE

- *Public IP address* indicates the address for accessing OBS.
- *xxx.xxx.xxx.xxx* indicates the IP address of the Direct Connect or VPN gateway created at your on-premises data center.
- The route command format varies depending on the OS. Use the route command format corresponding to the actual OS.

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 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.	● 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. – **BMS**: Backend resources of this type serve as servers. ● One VPC endpoint service corresponds to only one backend resource.
Viewing the Summary of a VPC Endpoint Service	Describes how to query details about a VPC endpoint service.	None
Deleting a VPC Endpoint Service	Describes how to delete a VPC endpoint service.	● 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.	● The VPC endpoint and the VPC endpoint service must be deployed in the same region. ● Before you configure the whitelist for a VPC endpoint service, obtain the 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.	● A port mapping needs to be configured when you create a VPC endpoint service. ● After a VPC endpoint service is created, you can view its port mappings but cannot modify them.
Managing Tags of a VPC Endpoint Service	Describes how to query, add, edit, and delete tags of a VPC endpoint service.	You can add up to 10 tags 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.
  - **BMS**: Backend resources of this type serve as servers.
- One VPC endpoint service corresponds to only one backend resource.

Prerequisites

There is a load balancer in the VPC where you are going to create the VPC endpoint service.

Procedure

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

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

Table 3-2 Parameters for creating a VPC endpoint service

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

Parameter	Description
Connection Approval	Specifies whether the connection between a VPC endpoint and a VPC endpoint service requires approval from the owner of the VPC endpoint service. You can enable or disable **Connection Approval**. When **Connection Approval** is enabled, any VPC endpoint for connecting to the VPC endpoint service needs to be approved. For details, see **Managing Connections of a VPC Endpoint Service**.
Port Mapping	Specifies the protocol and ports used for communications between the VPC endpoint service and a VPC endpoint. The protocol is TCP. ● **Service Port**: provided by the backend resource bound to the VPC endpoint service. ● **Terminal Port**: provided by the VPC endpoint, allowing you to access the VPC endpoint service. The service and terminal port numbers range from **1** to **65535**. A maximum of 50 port mappings can be added at a time. NOTE Accessing a VPC endpoint service from a VPC endpoint is to access the service port from the associated terminal port.
Backend Resource Type	Specifies the backend resource that provides services to be accessed. The following backend resource types are supported: ● **Elastic load balancer**: Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance. ● **ECS**: Backend resources of this type serve as servers. ● **BMS**: Backend resources of this type serve as servers. In this example, select **Elastic load balancer**. NOTE ● For the security group associated with the backend resource configured for the VPC endpoint service, add an inbound rule, with **Source** set to **198.19.128.0/17**. For details, see section "Adding a Security Group Rule" in the *Virtual Private Cloud User Guide*. ● If you configure a load balancer as the backend resource for the VPC endpoint service, and enable access control for the listener associated with the load balancer, ensure to allow traffic from 198.19.128.0/17.

Parameter	Description
Load Balancer	When **Backend Resource Type** is set to **Elastic load balancer**, select the load balancer that provides services from the drop-down list. **NOTE** If an elastic load balancer is used as the backend resource, the source IP address received by the VPC endpoint service is not the real address of the client.
ECS List	When **Backend Resource Type** is set to **ECS**, select an ECS from the ECS list.
BMS List	When **Backend Resource Type** is set to **BMS**, select a BMS from the BMS list. **NOTE** The BMS type will be discarded. The ELB type is recommended.
Tag	This parameter is optional. Specifies the VPC endpoint service tag, which consists of a key and a value. You can add up to 10 tags to each VPC endpoint service. Tag keys and values must meet requirements listed in **Table 3-3**.

Table 3-3 Tag requirements for VPC endpoint services

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

6. Click **Create Now**.
7. Click **Back to VPC Endpoint Service List** to view the newly-created VPC endpoint service.

3.3 Viewing the Summary of a VPC Endpoint Service

Scenarios

This section describes how to query the summary of a VPC endpoint service, including its 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. Click **Service List** and choose **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.

   – Search by tag.

     i. Click ︾ to the right of **Search by Tag**.

     ii. Enter a tag and a value.

     You can also 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**.

     VPC endpoint services containing the specified tag are displayed.

     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 its details.

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

Table 3-4 Parameters contained in the details of a VPC endpoint service

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 VPC where the VPC endpoint service is to be 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.
	Status	Specifies the status of the VPC endpoint. For details about statuses of VPC endpoint services and VPC endpoints, see **What Statuses Are There for a VPC Endpoint Service and VPC Endpoint?**
	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 option can be **Accept** or **Reject**.

Tab	Parameter	Description
Permission Management	Authorized Domain ID	Specifies the authorized domain ID for connecting to the VPC endpoint. The ID 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 communications between the VPC endpoint service and a 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.
Tags	Key	Specifies the tag key of the VPC endpoint service.
	Value	Specifies the tag value of the VPC endpoint service.
	Operation	Specifies the operation to be performed on the VPC endpoint service tag. You can click **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** state cannot be deleted.

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

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the required region and project.
3. Click **Service List** and choose **Networking** > **VPC Endpoint**.
4. In the VPC endpoint service list, locate the target VPC endpoint service and click **Delete** in the **Operation** column.
5. In the **Delete VPC Endpoint** dialog box, 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 VPC endpoint service.

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

Prerequisites

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

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the required region and project.
3. Click **Service List** and choose **Networking** > **VPC Endpoint**.
4. In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoint Services**.
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 from 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 or delete an authorized domain ID to and from the whitelist of the VPC 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.

Constraints

- The VPC endpoint and the VPC endpoint service must be deployed in the same region.
- Before you configure the whitelist for a VPC endpoint service, obtain the domain ID of the associated VPC endpoint.

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. Click **Service List** and choose **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.
   - *domain_id* indicates the ID of the authorized domain, for example, **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. Click **Service List** and choose **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, click 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. In the displayed **Delete from Whitelist** dialog box, 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.

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

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the required region and project.
3. Click **Service List** and choose **Networking** > **VPC Endpoint**.
4. In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoint Services**.
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 mappings configured for the VPC endpoint service are displayed.

3.8 Managing Tags of a VPC Endpoint Service

Scenarios

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

Tags help identify VPC endpoint services. You can add up to 10 tags to each VPC endpoint service.

Add a Tag

Perform the following operations to tag 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. Click **Service List** and choose **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 **Add Tag** dialog box, enter a key and a value.

   Table 3-5 describes the tag requirements.

   Table 3-5 Tag requirements for VPC endpoint services

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

9. Click **OK**.

Edit a Tag

Perform the following operations to edit a tag 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. Click **Service List** and choose **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 tag values.

9. Click **OK**.

Delete a Tag

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

CAUTION

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

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the required region and project.
3. Click **Service List** and choose **Networking** > **VPC Endpoint**.
4. In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoint Services**.
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.	● VPC endpoints are region-level resources. Select a region and project when you create such a VPC 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 the summary of a VPC endpoint.	A VPC endpoint supports a maximum of 3,000 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
Configuring Access Control for a VPC Endpoint	Describes how to enable access control for a VPC endpoint and configure a whitelist of IP addresses or CIDR blocks that are allowed to access the VPC endpoint.	● **Access Control** is only available for VPC endpoints for connecting to interface VPC endpoint services. ● If **Access Control** is disabled, any IP address can access the VPC endpoint. ● A maximum of 20 whitelist records can be added.
Managing Tags of a VPC Endpoint	Describes how to query, add, edit, and delete VPC endpoint tags.	You can add up to 10 tags 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 an interface or a gateway VPC endpoint based the type of the associated VPC endpoint service.

- **Creating a VPC Endpoint for Accessing Interface VPC Endpoint Services**
- **Creating a VPC Endpoint for Accessing Gateway VPC Endpoint Services**

Constraints

- VPC endpoints are region-level resources. Select a region and project when you create such a VPC 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.

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. Click **Service List** and choose **Networking** > **VPC Endpoint**.
4. On the **VPC Endpoints** page, click **Create VPC Endpoint**.
5. On the **Create VPC Endpoint** page, configure the parameters.

Table 4-2 VPC endpoint parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint is to be located. Resources in different regions cannot communicate with each other over an intranet. For lower latency and quicker access, select the nearest region.
Service Category	There are two options: ● **Cloud services**: Select this value if the target VPC endpoint service is a cloud service. ● **Find a service by name**: Select this value if the target VPC endpoint service is a private service of your own.
Service List	This parameter is available only when you select **Cloud services** for **Service Category**. The VPC endpoint service has been created by the O&M personnel and you can directly use it.
VPC Endpoint Service Name	This parameter is available only when you select **Find a service by name** for **Service Category**. In the VPC endpoint service list, locate the target VPC endpoint service, copy its name in the **Name** column, paste it to the **VPC Endpoint Service Name** text box, and click **Verify**. ● If "Service name found." is displayed, proceed with subsequent operations. ● If "Service name not found." is displayed, check whether the region is the same as that of the VPC endpoint service or whether the name entered is correct.
Create a Private Domain Name	If you want to access a VPC endpoint using a domain name, select **Create a Private Domain Name**. This parameter is mandatory when the VPC endpoint will be used to access an interface VPC endpoint service.
VPC	Specifies the VPC where the VPC endpoint is to be deployed.
Subnet	This parameter is available when you want to access an interface VPC endpoint service. Specifies the subnet where the VPC endpoint is to be located.

Parameter	Description
Private IP Address	This parameter is available when you want to access an interface VPC endpoint service. Specifies the private IP address of the VPC endpoint. You can select **Automatically assign** or **Manually specify**.
Access Control	This parameter is available when you want to access an interface VPC endpoint service. It controls IP addresses and CIDR blocks that are allowed to access the VPC endpoint. ● If **Access Control** is enabled, only IP addresses or CIDR blocks in the whitelist are allowed to access the VPC endpoint. ● If **Access Control** is disabled, any IP address or CIDR block can access the VPC endpoint.
Whitelist	This parameter is available when you want to access an interface endpoint service and **Access Control** is enabled. Lists the IP addresses or CIDR blocks that are allowed to access the VPC endpoint. You can add a maximum of 20 records.
Tag	This parameter is optional. Specifies the VPC endpoint tag, which consists of a key and a value. You can add up to 10 tags to each VPC endpoint. Tag keys and values must meet requirements listed in **Table 4-3**.

Table 4-3 Tag requirements for VPC endpoints

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

6. Confirm the specifications and click **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. Click **Service List** and choose **Networking** > **VPC Endpoint**.
4. On the **VPC Endpoints** page, click **Create VPC Endpoint**.
5. On the **Create VPC Endpoint** page, configure the parameters.

Table 4-4 VPC endpoint parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint is to be located. Resources in different regions cannot communicate with each other over an intranet. For lower latency and quicker access, select the nearest region.
Service Category	Specifies the type of services that are configured as gateway VPC endpoint services. Only cloud services are supported. Select **Cloud services**.
Service List	This parameter is available only when you select **Cloud services** for **Service Category**. In the VPC endpoint service list, select the VPC endpoint service whose type is gateway. The VPC endpoint service has been created by the O&M personnel and you can directly use it.
VPC	Specifies the VPC where the VPC endpoint is to be deployed.
Route Table	This parameter is available only when you create a VPC endpoint for connecting to a gateway VPC endpoint service. **NOTE** This parameter is available only in the regions where the route table function is enabled. You are advised to select all route tables. Otherwise, the access to OBS may fail. Select a route table required for the VPC where the VPC endpoint is to be located. For details about how to add routes, see the *Virtual Private Cloud User Guide*.

Parameter	Description
Tag	This parameter is optional. Specifies the VPC endpoint tag, which consists of a key and a value. You can add up to 10 tags to each VPC endpoint. Tag keys and values must meet requirements listed in **Table 4-5**.

Table 4-5 Tag requirements for VPC endpoints

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

6. Confirm the specifications and click **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.

Constraints

A VPC endpoint supports a maximum of 3,000 concurrent requests.

Querying a VPC Endpoint

Perform the following operations to query details about a VPC endpoint, including its 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. Click **Service List** and choose **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 **ID** or **VPC Endpoint Service Name** 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 tag.

     i. Click ︾ to the right of **Search by Tag**.

     ii. Enter a tag and a value.

     You can also 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 the ID of the target VPC endpoint to view its details.

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

Table 4-6 Parameters contained in the details of a VPC endpoint

Tab	Parameter	Description
Summary	ID	Specifies the ID of the VPC endpoint.
	VPC	Specifies the VPC where the VPC endpoint is deployed.
	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.

Tab	Parameter	Description
	Status	Specifies the status of the VPC endpoint.
	Type	Specifies the type of the VPC endpoint service that the VPC endpoint is used to access.
	Created	Specifies the creation time of the VPC endpoint.
	Access Control	Specifies whether the whitelist is enabled for IP addresses to access this VPC endpoint. ● If **Access Control** is enabled, only IP addresses or CIDR blocks in the whitelist are allowed to access the VPC endpoint. ● If **Access Control** is disabled, any IP address or CIDR block can access the VPC endpoint. **NOTE** Access control can be enabled only for VPC endpoints for connecting to an interface VPC endpoint service.
Access Control	IP Address or CIDR Block	It controls IP addresses and CIDR blocks that are allowed to access the VPC endpoint. **NOTE** The **Access Control** tab is displayed only for VPC endpoints for connecting to interface VPC endpoint services.
	Operation	Specifies the operation to be performed on whitelist records of the VPC endpoint. Only deletion is supported.
Route Table	Name	Specifies the name of the route table. **NOTE** The **Route Tables** tab is displayed only for the VPC endpoint for connecting to a gateway VPC endpoint service in some specific regions.
	VPC	Specifies the VPC that the route table belongs to.
	Type	Specifies the type of the route table, which can be **Default** and **Custom**.

Tab	Parameter	Description
	Associated Subnets	Specifies the number of subnets associated with the route table.
	Operation	Specifies the operation to be performed on the route table. The operation can be **Disassociate** or **Associate**. **NOTE** If a VPC endpoint is associated with only one route table, disassociation is not supported.
Tags	Key	Specifies the tag key of the VPC endpoint.
	Value	Specifies the tag value of the VPC endpoint.
	Operation	Specifies the operation to be performed on the VPC endpoint tag. You can click **Edit** or **Delete**.

Accessing a VPC Endpoint via Its Private IP Address

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

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

   Command Private IP address:*Port number*

   The following is a command example:

   curl *Private IP address:Port number*

Accessing a VPC Endpoint (via Its Private Domain Name)

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

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

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

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 Sets** page is displayed.

5. In the record set list, locate the target A record set and view its information.

   When **Status** changes to **Normal**, the resolution takes effect.

Accessing a VPC endpoint via its private domain name

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

   Command Private 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. Click **Service List** and choose **Networking** > **VPC Endpoint**.
4. In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoints**.
5. In the VPC endpoint list, locate the VPC endpoint to be deleted and click **Delete** in the **Operation** column.
6. In the **Delete VPC Endpoint** dialog box, click **Yes**.

4.5 Configuring Access Control for a VPC Endpoint

Scenarios

To control IP addresses and CIDR blocks that can access a VPC endpoint, configure a whitelist. You can add or delete a whitelist record, or disable access control if you no longer need it.

NOTE

- **Access Control** is only available for VPC endpoints for connecting to interface VPC endpoint services.
- If **Access Control** is disabled, any IP address can access the VPC endpoint.

For details about how to configure access control and whitelist when you are creating a VPC endpoint, see **Creating a VPC Endpoint**.

This section describes how to enable and configure access control after a VPC endpoint is created.

Constraints

- **Access Control** is only available for VPC endpoints for connecting to interface VPC endpoint services.
- If **Access Control** is disabled, any IP address can access the VPC endpoint.
- A maximum of 20 whitelist records can be added.

Enable Access Control and 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. Click **Service List** and choose **Networking** > **VPC Endpoint**.
4. In the VPC endpoint list, locate the target VPC endpoint and click its ID.
5. On the displayed page, click the **Access Control** tab.
6. On the **Access Control** tab, click **Add to Whitelist**.
7. Enter the authorized IP addresses or CIDR blocks.

   NOTE

   A maximum of 20 whitelist records can be added for each VPC endpoint.
8. Click **OK**.

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. Click **Service List** and choose **Networking** > **VPC Endpoint**.
4. In the VPC endpoint list, locate the target VPC endpoint and click its ID.
5. Select the **Access Control** tab.
6. In the whitelist, locate the target IP address or CIDR block and click **Delete** in the **Operation** column.

   To delete whitelist records, select all the target IP addresses or CIDR blocks and click **Delete** in the upper left corner.
7. In the displayed **Delete from Whitelist** dialog box, click **Yes**.

4.6 Managing Tags of a VPC Endpoint

Scenarios

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

Tags help identify VPC endpoints. You can add up to 10 tags to each VPC endpoint.

Add a Tag

Perform the following operations to tag 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. Click **Service List** and choose **Networking** > **VPC Endpoint**.
4. In the VPC endpoint list, locate the target VPC endpoint and click its ID.
5. On the displayed page, select the **Tags** tab.
6. Click **Add Tag**.
7. In the displayed **Add Tag** dialog box, enter a key and a value.
   Table 4-7 describes the tag requirements.

Table 4-7 Tag requirements for VPC endpoints

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

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. Click **Service List** and choose **Networking** > **VPC Endpoint**.
4. In the VPC endpoint list, locate the target VPC endpoint and click its ID.
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 tag 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. Click **Service List** and choose **Networking** > **VPC Endpoint**.
4. In the VPC endpoint list, locate the target VPC endpoint and click its ID.
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 Permissions Management

5.1 Creating a User and Granting VPC Endpoint Permissions

Use to implement fine-grained permissions control over your VPC Endpoint resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user has their own security credentials for accessing VPC Endpoint resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust an account or a cloud service to perform efficient O&M on your VPC Endpoint resources.

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

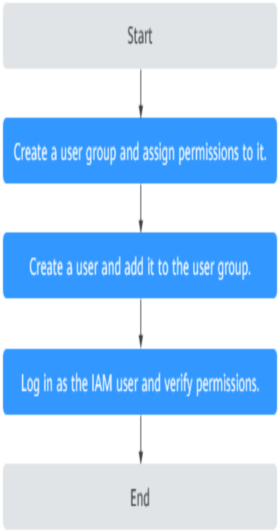
This section describes the process flow for granting permissions (see **Figure 5-1**).

Prerequisites

You must learn about permissions (see **Permissions**) supported by VPC Endpoint and choose policies or roles according to your requirements. To grant permissions for other services, learn about all **System Permissions** supported by IAM.

Process Flow

Figure 5-1 Process for granting VPC Endpoint permissions


Start
Create a user group and assign permissions to it.
Create a user and add it to the user group.
Log in as the IAM user and verify permissions.
End

1. **Create a user group and assign it permissions**.

   On the IAM console, create a user group and attach the policy to the group.

2. **Create an IAM user and add it to the created user group**.

   Create an IAM user and add it to the user group created in **1**.

3. **Log in as the IAM user** and verify permissions.

   In the authorized region, perform the following operations:

   - On the **Service List** page, choose **VPC Endpoint**. Click **Create VPC Endpoint** in the upper right corner. If you can create a VPC endpoint, the **VPCEndpoint Administrator** policy has already taken effect.
   - Choose another service from **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **VPCEndpoint Administrator** policy has already taken effect.

6 Quotas

What Is Quota?

Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. In the upper right corner of the page, click 📊 .

   The **Service Quota** page is displayed.
3. View the used and total quota of each type of resources on the displayed page.

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

How Do I Apply for a Higher Quota?

The system does not support online quota adjustment.

If you need to adjust a quota, contact the operations administrator.

7 FAQ

7.1 What Should I Do If the VPC Endpoint I Purchased Cannot Connect to a 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 198.19.128.0/17 CIDR block in the inbound direction. If it does not, add inbound rules for this CIDR block 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.
3. If you configure a load balancer as the backend resource for the VPC endpoint service, and enable access control for the listener associated with the load balancer, ensure to allow traffic from 198.19.128.0/17.

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

Table 7-1 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 7-1 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.
Communications 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, 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.
Access using VPN/Direct Connect	Supported You can create a VPC Peering connection to connect your on-premises data center to a cloud service using a VPN connection or a direct connection.	Supported You can create a VPC endpoint to connect your on-premises data center to a cloud service using a VPN connection or a direct connection over an internal network.

7.3 What Statuses Are There for a VPC Endpoint Service and VPC Endpoint?

Table 7-2 describes statuses of a VPC endpoint service and their meanings.

Table 7-2 Statuses of a VPC endpoint service

Status	Description
Creating	Indicates that the VPC endpoint service is being created.

Status	Description
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 7-3 describes statuses of a VPC endpoint and their meanings.

Table 7-3 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.
Failed	Indicates that the VPC endpoint fails to connect to the associated VPC endpoint service.
Deleting	Indicates that the VPC endpoint is being deleted.

7.4 Does VPC Endpoint Support Cross-Region Access?

VPC endpoint services cannot be accessed across regions. VPC Endpoint supports only access to cloud services or users' private services in VPCs in the same region.

A Change History

Released On	Description
2020-12-11	This issue is the first official release.