

**VPC Endpoint**

# **User Guide (Ankara Region)**

**Issue** 01  
**Date** 2024-04-12



**Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.**

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

## **Trademarks and Permissions**



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

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

## **Notice**

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

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

# 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

---

<b>1 Service Overview</b>	<b>1</b>
1.1 What Is VPC Endpoint?	1
1.2 Product Advantages	2
1.3 Application Scenarios	2
1.4 Constraints	3
1.5 VPC Endpoint and Other Services	3
1.6 Permissions	4
1.7 Product Concepts	7
1.7.1 VPC Endpoint Services	7
1.7.2 VPC Endpoints	8
1.7.3 User Permissions	9
1.7.4 Region and AZ	9
<b>2 Getting Started</b>	<b>11</b>
2.1 Operation Guide	11
2.2 Configuring a VPC Endpoint for Communications Across VPCs of the Same Account	11
2.2.1 Overview	12
2.2.2 Step 1: Create a VPC Endpoint Service	13
2.2.3 Step 2: Create a VPC Endpoint	15
2.3 Configuring a VPC Endpoint for Communications Across VPCs of Different Accounts	17
2.3.1 Overview	17
2.3.2 Step 1: Create a VPC Endpoint Service	19
2.3.3 Step 2: Add a Whitelist Record	21
2.3.4 Step 3: Create a VPC Endpoint	22
<b>3 VPC Endpoint Services</b>	<b>24</b>
3.1 VPC Endpoint Service Overview	24
3.2 Creating a VPC Endpoint Service	26
3.3 Viewing the Summary of a VPC Endpoint Service	29
3.4 Deleting a VPC Endpoint Service	31
3.5 Managing Connections of a VPC Endpoint Service	31
3.6 Managing Whitelist Records of a VPC Endpoint Service	32
3.7 Viewing Port Mappings of a VPC Endpoint Service	33
<b>4 VPC Endpoints</b>	<b>35</b>

---

4.1 VPC Endpoint Overview.....	35
4.2 Creating a VPC Endpoint.....	36
4.3 Querying and Accessing a VPC Endpoint.....	38
4.4 Deleting a VPC Endpoint.....	39
<b>5 Permissions Management.....</b>	<b>41</b>
5.1 Creating a User and Granting VPC Endpoint Permissions.....	41
5.2 Creating a Custom Policy.....	42
<b>6 Quotas.....</b>	<b>47</b>
<b>7 FAQ.....</b>	<b>48</b>
7.1 What Should I Do If the VPC Endpoint I Purchased Cannot Connect to a VPC Endpoint Service?.....	48
7.2 What Are the Differences Between VPC Endpoints and VPC Peering Connections?.....	48
7.3 What Statuses Are Available for a VPC Endpoint Service and VPC Endpoint?.....	49
7.4 Does VPC Endpoint Support Cross-Region Access?.....	50
<b>A Change History.....</b>	<b>51</b>

# 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](#).

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

### Accessing VPC Endpoint

You can access VPC Endpoint using any of the following:

- Huawei Cloud management 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, meeting requirements in different service scenarios.
- **Ready to Use:** 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.

### Cross-VPC Connection

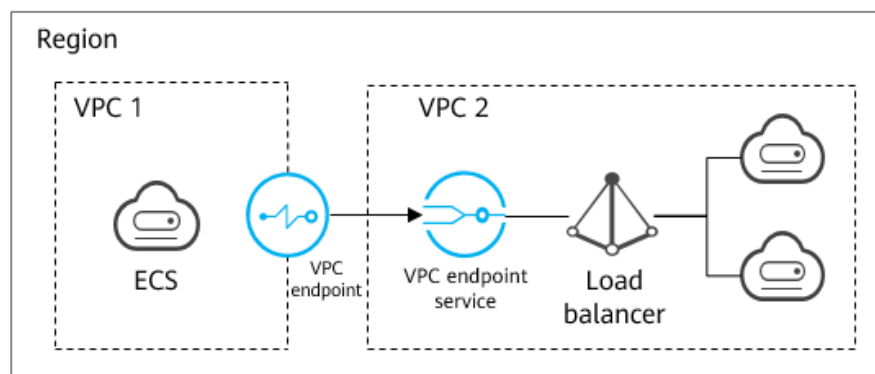
VPC Endpoint enables your resources in two different VPCs within a region to communicate with each other.

#### 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 Endpoint and VPC Peering Connections?" in the *VPC Endpoint User Guide*.

**Figure 1-1** Cross-VPC connection



**Figure 1-1** shows how an ECS in VPC 1 uses a VPC endpoint to access a load balancer in VPC 2 over a private network.

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 Account
- Configuring a VPC Endpoint for Communications Across VPCs of Different Accounts

## 1.4 Constraints

### Resource Quotas

**Table 1-1** describes quotas and constraints on VPC Endpoint resources.

**Table 1-1** VPC Endpoint resource quotas and constraints

Resource	Default Quota and Constraints	How to Increase Quota
VPC endpoint services per account in one region	20	"Quota Adjustment" in the <i>VPC Endpoint User Guide</i>
VPC endpoints per account in one region	50	"Quota Adjustment" in the <i>VPC Endpoint User Guide</i>

### Other Constraints

- When you create a VPC endpoint, ensure that the associated VPC endpoint service is deployed 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 can have 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	In the VPC Endpoint <i>Getting Started</i> : <ul style="list-style-type: none"> <li>Configuring a VPC Endpoint for Communications Across VPCs of the Same Account</li> <li>Configuring a VPC Endpoint for Communications Across VPCs of Different Accounts</li> </ul>
Creating IAM users and controlling their access to VPC Endpoint 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	Section "Creating a VPC Endpoint" in the <i>VPC Endpoint User Guide</i>
Configuring a private service as a VPC endpoint service. You can create a VPC endpoint to access the VPC endpoint service.	ELB	Section "Creating a VPC Endpoint Service" in the <i>VPC Endpoint User Guide</i>
	ECS	

## 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 *Identity and Access Management User Guide*.

## 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.

You can grant permissions by using roles or policies.

- **Roles:** A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. Only a limited number of service-level roles are available for authorization. Cloud services depend on each other. When you grant permissions using roles, you also need to attach any existing role dependencies. Roles are not ideal for fine-grained authorization and least privilege access.
- **Policies:** A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant users only the permissions to manage a certain type of VPC Endpoint resources. Most fine-grained policies contain permissions for specific APIs. For the API actions supported by VPC Endpoint, see "Permissions Policies and Supported Actions" in *VPC Endpoint API Reference*.

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

**Table 1-3** System-defined permissions for VPC Endpoint

Role/Policy Name	Description	Type	Dependency
VPCEP Administrator	Full permissions for VPC Endpoint	System-defined role	This role depends on <b>Server Administrator</b> , and <b>VPC Administrator</b> roles in the same project.
VPCEndpoint FullAccess	Full permissions for VPC Endpoint	System-defined policy	None

Role/Policy Name	Description	Type	Dependency
VPCEndpointReadOnlyAccess	Read-only permissions for VPC Endpoint. Users with these permissions can only view VPC Endpoint resources.	System-defined policy	None

**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	VPCEndpointFull Access	VPCEndpointReadOnlyAccess	VPCEP Administrator
Creating a VPC endpoint service	√	x	√
Deleting a VPC endpoint service	√	x	√
Querying a VPC endpoint service	√	√	√
Modifying a VPC endpoint service	√	x	√
Accepting or rejecting a VPC endpoint for a VPC endpoint service	√	x	√
Adding or removing a whitelist record	√	x	√
Creating a VPC endpoint	√	x	√
Deleting a VPC endpoint	√	x	√
Modifying a VPC endpoint	√	x	√

Operation	VPCEndpointFull Access	VPCEndpointReadOnlyAccess	VPCEP Administrator
Querying a VPC endpoint	√	√	√
Configuring access control for a VPC endpoint	√	x	√

## Helpful Links

- Section "Creating a User and Granting Permissions" in the *VPC Endpoint User Guide*

## Related References

- *Identity and Access Management User Guide*
- Section "Creating a Custom Policy" in the *VPC Endpoint User Guide*
- Section "Permissions Policies and Supported Actions" in the *VPC Endpoint API Reference*.

# 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. Cloud services are configured as VPC endpoint services by the O&M personnel by default. However, you need to create VPC endpoint services for your private services.

### 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	None	Access OBS using its private address.

## Interface VPC Endpoint Services

Interface VPC endpoint services are mainly configured from:

- Cloud services. You do not have the 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	None	VPC endpoint services enable you to access DNS over private networks.
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.

### 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

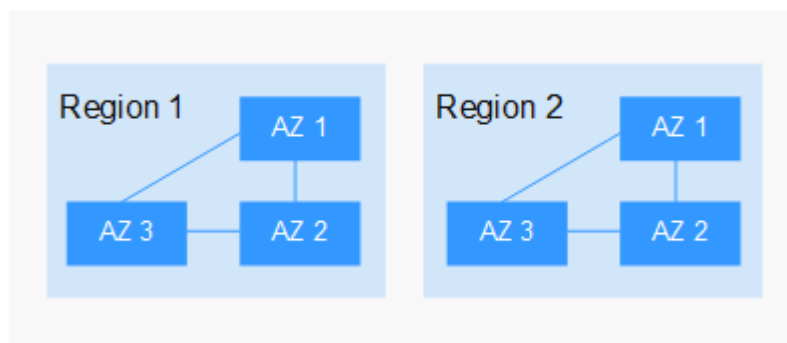
#### Concept

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 1-2** shows the relationship between regions and AZs.

**Figure 1-2** 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: <ul style="list-style-type: none"><li>• <a href="#">Configuring a VPC Endpoint for Communications Across VPCs of the Same Account</a></li><li>• <a href="#">Configuring a VPC Endpoint for Communications Across VPCs of Different Accounts</a></li></ul>

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



## 2.2.1 Overview

### Scenarios

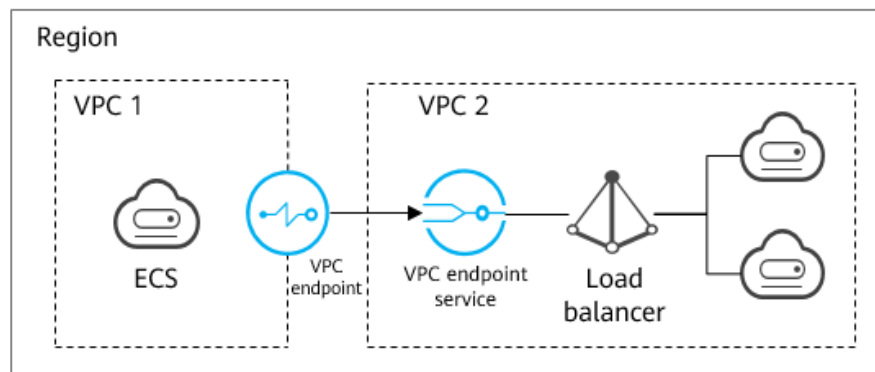
With VPC Endpoint, you can access resources across VPCs in the same region.

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 account in the same region can communicate with each other.

VPC 1 and VPC 2 belong to the same account in the same region. You can configure ELB in VPC 2 as a VPC endpoint service and 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



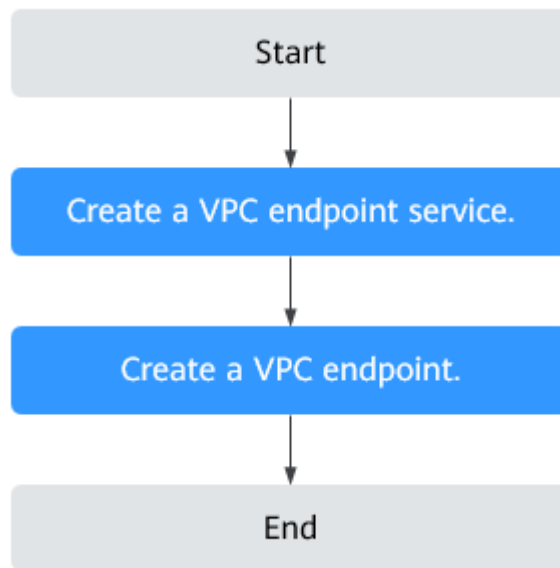
#### NOTE

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

### Configuration Process

**Figure 2-2** shows how to enable communications between VPCs of the same account 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	<p>Specifies the region where the VPC endpoint service is to be deployed.</p> <p>Resources in different regions cannot communicate with each other over an intranet. For lower latency and quicker access, select the nearest region.</p>
VPC	<p>Specifies the VPC where the VPC endpoint service is to be deployed.</p>
Service Type	<p>Specifies the type of the VPC endpoint service. The type can only be <b>Interface</b>.</p>
Connection Approval	<p>Specifies whether the connection between a VPC endpoint and a VPC endpoint service requires approval from the owner of the VPC endpoint service.</p> <p>You can enable or disable <b>Connection Approval</b>.</p> <p>When <b>Connection Approval</b> is enabled, any VPC endpoint for connecting to the VPC endpoint service needs to be approved. For details, see step 7.</p>
Port Mapping	<p>Specifies the protocol and ports used for communications between the VPC endpoint service and a VPC endpoint. The protocol is TCP.</p> <ul style="list-style-type: none"><li>• <b>Service Port:</b> provided by the backend resource bound to the VPC endpoint service.</li><li>• <b>Terminal Port:</b> provided by the VPC endpoint, allowing you to access the VPC endpoint service.</li></ul> <p>The service and terminal port numbers range from <b>1</b> to <b>65535</b>. A maximum of 50 port mappings can be added at a time.</p> <p><b>NOTE</b> Accessing a VPC endpoint service from a VPC endpoint is to access the service port from the associated terminal port.</p>

Parameter	Description
Backend Resource Type	<p>Specifies the backend resource that provides services to be accessed.</p> <p>The following backend resource types are supported:</p> <ul style="list-style-type: none"> <li>• <b>Elastic load balancer:</b> Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance.</li> <li>• <b>ECS:</b> Backend resources of this type serve as servers.</li> </ul> <p>In this example, select <b>Elastic load balancer</b>.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• For the security group associated with the backend resource configured for the VPC endpoint service, add an inbound rule, with <b>Source</b> set to <b>198.19.128.0/17</b>. For details, see section "Adding a Security Group Rule" in the <i>Virtual Private Cloud User Guide</i>.</li> <li>• 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.</li> </ul>
Load Balancer	<p>When <b>Backend Resource Type</b> is set to <b>Elastic load balancer</b>, select the load balancer that provides services from the drop-down list.</p> <p><b>NOTE</b></p> <p>If an elastic load balancer is used as the backend resource, the source IP address received by the VPC endpoint service is not the real address of the client.</p>

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 2-3** VPC endpoint parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint is to be located. This region is the same as that of the VPC endpoint service.
Service Category	There are two options: <ul style="list-style-type: none"><li>● <b>Cloud services</b>: Select this value if the target VPC endpoint service is a cloud service.</li><li>● <b>Find a service by name</b>: Select this value if the target VPC endpoint service is a private service of your own.</li></ul> In this example, select <b>Find a service by name</b> .
VPC Endpoint Service Name	This parameter is available only when you select <b>Find a service by name</b> for <b>Service Category</b> . Enter the VPC endpoint service name recorded in step <a href="#">88</a> , and click <b>Verify</b> . <ul style="list-style-type: none"><li>● If "Service name found." is displayed, proceed with subsequent operations.</li><li>● 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.</li></ul>
VPC	Specifies the VPC where the VPC endpoint is to be deployed.
Subnet	Specifies the subnet where the VPC endpoint is to be located.

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.

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 10.0.0.231
[root@ ~]# ssh -p 50 172.17.0.149
The authenticity of host '[172.17.0.149]:50 ([172.17.0.149]:50)' can't be established.
ECDSA key fingerprint is SHA256:4P811W6CBbsNE0P09tI02M4pBaPigH8yjN+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 Accounts

### 2.3.1 Overview

#### Scenarios

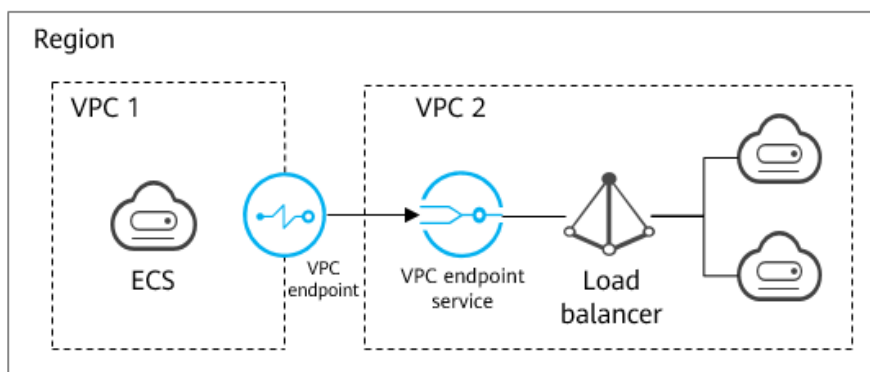
With VPC Endpoint, you can access resources across VPCs in the same region.

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 accounts in the same region can communicate with each other.

VPC 1 and VPC 2 belong to different accounts. You can configure ELB in VPC 2 as a VPC endpoint service and 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



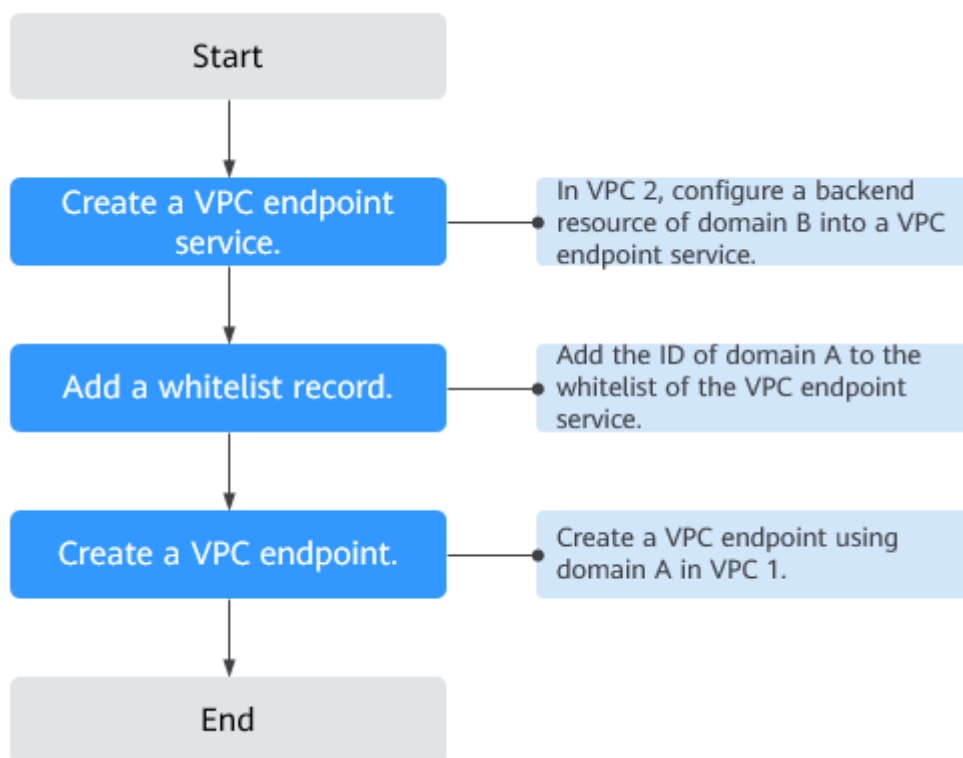
**NOTE**

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

## Cross-VPC Communications

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

Figure 2-5 Cross-VPC communications flowchart



## 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 account 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 2-4** 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.
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 <b>Interface</b> .
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 <b>Connection Approval</b> . When <b>Connection Approval</b> is enabled, any VPC endpoint for connecting to the VPC endpoint service needs to be approved. For details, see step 7.



Parameter	Description
Port Mapping	<p>Specifies the protocol and ports used for communications between the VPC endpoint service and a VPC endpoint. The protocol is TCP.</p> <ul style="list-style-type: none"> <li>• <b>Service Port:</b> provided by the backend resource bound to the VPC endpoint service.</li> <li>• <b>Terminal Port:</b> provided by the VPC endpoint, allowing you to access the VPC endpoint service.</li> </ul> <p>The service and terminal port numbers range from <b>1</b> to <b>65535</b>. A maximum of 50 port mappings can be added at a time.</p> <p><b>NOTE</b> Accessing a VPC endpoint service from a VPC endpoint is to access the service port from the associated terminal port.</p>
Backend Resource Type	<p>Specifies the backend resource that provides services to be accessed.</p> <p>The following backend resource types are supported:</p> <ul style="list-style-type: none"> <li>• <b>Elastic load balancer:</b> Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance.</li> <li>• <b>ECS:</b> Backend resources of this type serve as servers.</li> </ul> <p>In this example, select <b>Elastic load balancer</b>.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• For the security group associated with the backend resource configured for the VPC endpoint service, add an inbound rule, with <b>Source</b> set to <b>198.19.128.0/17</b>. For details, see section "Adding a Security Group Rule" in the <i>Virtual Private Cloud User Guide</i>.</li> <li>• 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.</li> </ul>
Load Balancer	<p>When <b>Backend Resource Type</b> is set to <b>Elastic load balancer</b>, select the load balancer that provides services from the drop-down list.</p> <p><b>NOTE</b> If an elastic load balancer is used as the backend resource, the source IP address received by the VPC endpoint service is not the real address of the client.</p>

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 account to a VPC endpoint service in another.

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

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

### Prerequisites

The required VPC endpoint service is available.


### Constraints

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

### Obtain the ID of Your Own Account

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

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

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

#### NOTE

- Your account is in the whitelist of your VPC endpoint service by default.
- The authorized account ID is in the **iam:domain::domain\_id** format.  
*domain\_id* indicates the ID of the authorized account, for example, **iam:domain::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 2-5** 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.
Service Category	There are two options: <ul style="list-style-type: none"> <li>• <b>Cloud services:</b> Select this value if the target VPC endpoint service is a cloud service.</li> <li>• <b>Find a service by name:</b> Select this value if the target VPC endpoint service is a private service of your own.</li> </ul> In this example, select <b>Find a service by name</b> .
VPC Endpoint Service Name	This parameter is available only when you select <b>Find a service by name</b> for <b>Service Category</b> . Enter the VPC endpoint service name recorded in step <b>88</b> , and click <b>Verify</b> . <ul style="list-style-type: none"> <li>• If "Service name found." is displayed, proceed with subsequent operations.</li> <li>• 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.</li> </ul>
VPC	Specifies the VPC where the VPC endpoint is to be deployed.
Subnet	Specifies the subnet where the VPC endpoint is to be located.

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.

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

# 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. Cloud services are configured as VPC endpoint services by the O&M personnel by default. However, you need to create VPC endpoint services for your private services.

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

Operation	Description	Constraint
<a href="#">Managing Connections of a VPC Endpoint Service</a>	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.
<a href="#">Managing Whitelist Records of a VPC Endpoint Service</a>	Describes how to manage whitelist records of a VPC endpoint service to control across-account access between a VPC endpoint and a VPC endpoint service.	<ul style="list-style-type: none"> <li>The VPC endpoint and the VPC endpoint service must be deployed in the same region.</li> <li>Before you configure the whitelist for a VPC endpoint service, obtain the account ID of the associated VPC endpoint.</li> </ul>
<a href="#">Viewing Port Mappings of a VPC Endpoint Service</a>	Describes how to view the port mapping between a VPC endpoint and a VPC endpoint service, including the supported protocol, service port, and terminal port.	<ul style="list-style-type: none"> <li>A port mapping needs to be configured when you create a VPC endpoint service.</li> <li>After a VPC endpoint service is created, you can view its port mappings but cannot modify them.</li> </ul>

## 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. Cloud services are configured as VPC endpoint services by the O&M personnel by default. However, you need to create VPC endpoint services for your private services.

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

### Constraints


- VPC endpoint services are region-level resources. Select a region and project when you create such a service.
- Each tenant can create a maximum of 20 VPC endpoint services.
- The following private services can be configured into VPC endpoint services:
  - Elastic load balancer:** Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance.

- **ECS**: Backend resources of this type serve as servers.
- One VPC endpoint service corresponds to only one backend resource.

## Prerequisites

There 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.
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 <b>Interface</b> .
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 <b>Connection Approval</b> .  When <b>Connection Approval</b> is enabled, any VPC endpoint for connecting to the VPC endpoint service needs to be approved. For details, see <a href="#">Managing Connections of a VPC Endpoint Service</a> .



Parameter	Description
Port Mapping	<p>Specifies the protocol and ports used for communications between the VPC endpoint service and a VPC endpoint. The protocol is TCP.</p> <ul style="list-style-type: none"> <li>• <b>Service Port:</b> provided by the backend resource bound to the VPC endpoint service.</li> <li>• <b>Terminal Port:</b> provided by the VPC endpoint, allowing you to access the VPC endpoint service.</li> </ul> <p>The service and terminal port numbers range from <b>1</b> to <b>65535</b>. A maximum of 50 port mappings can be added at a time.</p> <p><b>NOTE</b> Accessing a VPC endpoint service from a VPC endpoint is to access the service port from the associated terminal port.</p>
Backend Resource Type	<p>Specifies the backend resource that provides services to be accessed.</p> <p>The following backend resource types are supported:</p> <ul style="list-style-type: none"> <li>• <b>Elastic load balancer:</b> Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance.</li> <li>• <b>ECS:</b> Backend resources of this type serve as servers.</li> </ul> <p>In this example, select <b>Elastic load balancer</b>.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• For the security group associated with the backend resource configured for the VPC endpoint service, add an inbound rule, with <b>Source</b> set to <b>198.19.128.0/17</b>. For details, see section "Adding a Security Group Rule" in the <i>Virtual Private Cloud User Guide</i>.</li> <li>• 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.</li> </ul>
Load Balancer	<p>When <b>Backend Resource Type</b> is set to <b>Elastic load balancer</b>, select the load balancer that provides services from the drop-down list.</p> <p><b>NOTE</b> If an elastic load balancer is used as the backend resource, the source IP address received by the VPC endpoint service is not the real address of the client.</p>
ECS List	<p>When <b>Backend Resource Type</b> is set to <b>ECS</b>, select an ECS from the ECS list.</p>


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**.
5. In the VPC endpoint service list, locate the target VPC endpoint service and click its name to view its details.

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

**Table 3-3** 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.	

Tab	Parameter	Description
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 <a href="#">What Statuses Are Available for a VPC Endpoint Service and VPC Endpoint?</a>
	Owner	Specifies the account 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 <b>Accept</b> or <b>Reject</b> .
Permission Management	Authorized Account ID	Specifies the authorized account 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 account 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.

## 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 Available 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 account to a VPC endpoint service in another.

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

- If the whitelist is empty, access from a VPC endpoint in another account is not allowed.
- If an authorized account ID is already in the whitelist, you can use this account to create a VPC endpoint for connecting to the VPC endpoint service.
- If an authorized account ID is not in the whitelist, you cannot use this account 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 account 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 account ID in the required format and click **OK**.

 **NOTE**

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

## Delete a Whitelist Record


1. Log in to the management console.
2. Click  in the upper left corner and select the required region and project.
3. 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 account ID, and click **Delete** in the **Operation** column.  
To delete multiple whitelist records, select all the target account 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.

# 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
<a href="#">Creating a VPC Endpoint</a>	Describes how to create a VPC endpoint.	<ul style="list-style-type: none"><li>• VPC endpoints are region-level resources. Select a region and project when you create such a VPC endpoint.</li><li>• Each tenant can create a maximum of 50 VPC endpoints.</li><li>• When you create a VPC endpoint, ensure that the associated VPC endpoint service is deployed in the same region as the VPC endpoint.</li></ul>
<a href="#">Querying and Accessing a VPC Endpoint</a>	Describes how to query the summary of a VPC endpoint.	A VPC endpoint supports a maximum of 3,000 concurrent requests.
<a href="#">Deleting a VPC Endpoint</a>	Describes how to delete a VPC endpoint.	Deleted VPC endpoints cannot be recovered. Exercise caution when performing this operation.



## 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 is deployed 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.

Parameter	Description
Service Category	There are two options: <ul style="list-style-type: none"> <li>• <b>Cloud services:</b> Select this value if the target VPC endpoint service is a cloud service.</li> <li>• <b>Find a service by name:</b> Select this value if the target VPC endpoint service is a private service of your own.</li> </ul>
Service List	This parameter is available only when you select <b>Cloud services</b> for <b>Service Category</b> . 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 <b>Find a service by name</b> for <b>Service Category</b> . In the VPC endpoint service list, locate the target VPC endpoint service, copy its name in the <b>Name</b> column, paste it to the <b>VPC Endpoint Service Name</b> text box, and click <b>Verify</b> . <ul style="list-style-type: none"> <li>• If "Service name found." is displayed, proceed with subsequent operations.</li> <li>• 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.</li> </ul>
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.

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 4-3** VPC endpoint parameters

Parameter	Description
Region	Specifies the region where the VPC endpoint is to be located. Resources in different regions cannot communicate with each other over an intranet. For lower latency and quicker access, select the nearest region.
Service Category	Specifies the type of services that are configured as gateway VPC endpoint services. Only cloud services are supported. Select <b>Cloud services</b> .
Service List	This parameter is available only when you select <b>Cloud services</b> for <b>Service Category</b> . 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.

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**.
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.

**Table 4-4** 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.
	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.

## 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*

## 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**.

# 5 Permissions Management

---

## 5.1 Creating a User and Granting VPC Endpoint Permissions

Use IAM 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.

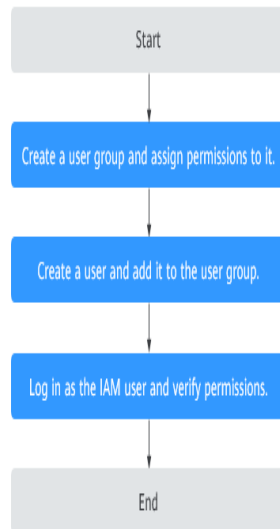
This section describes the process flow for granting permissions (see [Figure 5-1](#)).

### 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



1. Create a user group and assign it permissions.  
On the IAM console, create a user group, choose **Authorize** in the **Operation** column, and attach the **VPCEP Administrator** policy to the group.
2. Create an IAM user and add it to the created user group.  
Create a user on the IAM console and add it to the user group created in **1** by choosing **Authorize** in the **Operation** column.
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 **VPCEP 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 **VPCEP Administrator** policy has already taken effect.

## 5.2 Creating a Custom Policy

You can create custom policies to supplement system-defined policies and implement more refined access control.

You can create custom policies in either of the following two ways:

- Visual editor: Select cloud services, actions, resources, and request conditions without the need to know policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

The following describes how to create a custom policy that allows users to modify VPC endpoint service policies in the visual editor and JSON view.

This section provides examples of common custom VPC Endpoint policies.

## Creating a Custom Policy in the Visual Editor

1. Log in to the management console.
2. Choose **Management & Deployment > Identity and Access Management**.  
The IAM console is displayed.
3. In the left navigation pane, choose **Policies**.
4. Click **Create Custom Policy**.  
The **Create Custom Policy** page is displayed.
5. Enter a policy name.
6. Select a scope in which the policy will take effect based on the type of services to be set in this policy.
  - **Global:** Select this option if the services to which the policy is related must be deployed in the Global region. When creating custom policies for globally deployed services, specify the scope as **Global services**. Custom policies of this scope must be attached to user groups for global services.
  - **Project-level:** Select this option if the services to which the policy is related must be deployed in specific regions. When creating custom policies for regionally deployed services, specify the scope as **Project-level services**. Custom policies of this scope must be attached to user groups for specific projects except the global service project.

Select **Project-level services** here.

### NOTE

A custom policy can contain actions of multiple services that are globally accessible or accessible through region-specific projects. To define permissions required to access both global and project-level services, create two custom policies and specify the scope as **Global services** and **Project-level services**.

7. Select **Visual editor** for **Policy View**.
8. In the **Policy Content** area, configure a custom policy.
  - a. Select **Allow** or **Deny**.
  - b. Select **Cloud service**.

### NOTE

Only one cloud service can be selected for each permission block. To configure permissions for cloud services, click **Add Permissions** or refer to [Creating a Custom Policy in the JSON View](#).

- c. Select actions.
- d. (Optional) Select a resource type. For example, if you select **Specific**, you can click **Specify resource path** to specify the resource to be authorized.
- e. (Optional) Add request conditions by specifying condition keys, operators, and values.



**Table 5-1** Criterion

Parameter	Description
Condition Key	<p>Specifies a key in the <b>Condition</b> element of a statement. There are global and service-level condition keys.</p> <ul style="list-style-type: none"> <li>Global-level condition key: The prefix is <b>g</b>, which is applicable to all operations, as shown in <a href="#">Table 5-2</a>.</li> <li>Project-level condition key: The prefix is the abbreviation of a service, for example, <b>vpcep</b>. This key applies only to operations of the corresponding service.</li> </ul>
Operator	An operator must be used together with a condition key to form a complete condition statement.
Value	A value is used together with a condition key and an operator that requires a keyword, to form a complete condition statement.

**Table 5-2** Global request condition

Global Condition Key	Type	Description
g:CurrentTime	Time	Specifies when an authentication request was received. The time is in ISO 8601 format, for example, <b>2012-11-11T23:59:59Z</b> .
g:DomainName	String	Specifies the account name.
g:MFAPresent	Boolean	Specifies whether to use multi-factor authentication (MFA) to obtain a token.
g:MFAAge	Value	Specifies the validity period of the token obtained through MFA. This condition must be used together with <b>g:MFAPresent</b> .
g:ProjectName	String	Specifies the project name.

Global Condition Key	Type	Description
g:ServiceName	String	Specifies the service name.
g:UserId	String	Specifies the IAM user ID.
g:Username	String	Specifies the IAM username.

9. (Optional) Switch to the JSON view and modify the policy content in JSON format.

 **NOTE**

If the policy content is incorrect after modification, check and modify the content, or click **Reset** to cancel the modifications.

10. (Optional) To add another permission block for the policy, click **Add Permissions**. Alternatively, click the plus (+) icon on the right of an existing permission block to clone its permissions.
11. (Optional) Describe the policy.
12. Click **OK**.
13. Assign the policy to a user group. Users in the group can inherit the permissions of the policy by referring to [Creating a User and Granting VPC Endpoint Permissions](#).

## Creating a Custom Policy in the JSON View

1. Log in to the management console.
2. Choose **Management & Deployment > Identity and Access Management**.  
The IAM console is displayed.
3. In the left navigation pane, choose **Policies**.
4. Click **Create Custom Policy**.  
The **Create Custom Policy** page is displayed.
5. Enter a policy name.
6. Select a scope in which the policy will take effect based on the type of services to be set in this policy.
  - **Global:** Select this option if the services to which the policy is related must be deployed in the Global region. When creating custom policies for globally deployed services, specify the scope as **Global services**. Custom policies of this scope must be attached to user groups for global services.
  - **Project-level:** Select this option if the services to which the policy is related must be deployed in specific regions. When creating custom policies for regionally deployed services, specify the scope as **Project-level services**. Custom policies of this scope must be attached to user groups for specific projects except the global service project.

Select **Project-level services** here.

 **NOTE**

A custom policy can contain actions of multiple services that are globally accessible or accessible through region-specific projects. To define permissions required to access both global and project-level services, create two custom policies and specify the scope as **Global services** and **Project-level services**.

7. Select **JSON** for **Policy View**.
8. (Optional) Click **Select Existing Policy**, and select a policy to use it as template, such as **VPCEndpoint FullAccess**.
9. Click **Yes**.
10. Modify the statements in the template.
  - **Effect**: Set it to **Allow** or **Deny**.
  - **Action**: Enter the actions listed in the VPC Endpoint API actions table, for example, **vpcep:epservices:update**.

 **NOTE**

The version of each custom policy is fixed at **1.1**.

11. (Optional) Describe the policy.
12. Click **OK**.

If the policy list is displayed, the policy was created successfully. If a message indicating incorrect policy content is displayed, modify the policy.
13. Assign the policy to a user group.

Users in the group can inherit the permissions of the policy by referring to [Creating a User and Granting VPC Endpoint Permissions](#).

# 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.

Before contacting the operations administrator, make sure that the following information has been obtained:

- Account name, which can be obtained by performing the following operations:  
Log in to the management console using the cloud account, click the username in the upper right corner, select **My Credentials** from the drop-down list, and obtain the account name on the **My Credentials** page.
- Quota information, which includes service name, quota type, and required quota

# 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.

## 7.3 What Statuses Are Available 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.
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
2024-04-12	This issue is the first official release.