VPC Endpoint (VPCEP)
8.2.1
User Guide

Issue	02
Date	2023-04-30

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property 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 Cloud 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.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Introduction

1.1 What Is VPC Endpoint?

Definition

VPC Endpoint (VPCEP) is a cloud service that extends VPC capabilities. It provides secure and private channels to connect VPCs to endpoint services, providing powerful and flexible networking without having to use EIPs.

Resource Composition

VPCEP consists of endpoint services and endpoints that are created by service providers and users respectively.

- Endpoint services: Currently, your private services are supported. You can create an application on a cloud server in your VPC and configure it as an endpoint service.
- Endpoints: Endpoints are channels for connecting VPCs to endpoint services. You can create an application in your VPC and configure it as an endpoint service. In the same region, you can create an endpoint in another VPC and then use this endpoint to access the endpoint service.

Figure 1-1 Resource Composition

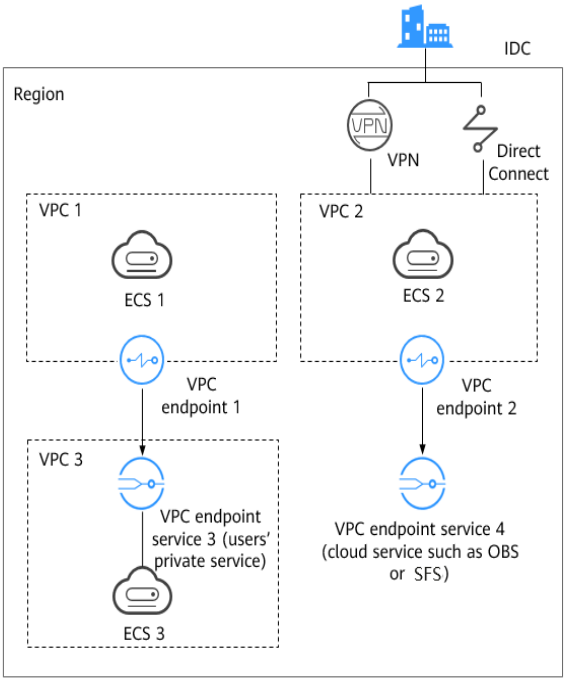


Figure 1-1 shows the process of establishing channels for network communications between:

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

1.2 Advantages

With an endpoint, you can securely and easily access endpoint services in VPCs.

- Secure access

  An endpoint service provides services in a VPC to resources in another VPC, enabling point-to-point unidirectional access across VPCs while exposing no server-related network information. The endpoint service makes your access more secure and reliable.

- Convenient connection

  An endpoint provides an easy-to-use, secure, and dedicated channel for a VPC to connect to endpoint services, such as cloud services and users' private services. The endpoint service uses an internal network and requires no EIP or NAT gateway, providing a more powerful and flexible network.

- Simple operation

  An endpoint service provider can create an application in a VPC and configure it as an endpoint service. Other users can use endpoints to create connections between their VPCs and the endpoint service of the service provider.

1.3 Application Scenarios

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

You can use VPCEP in different scenarios.

High-Speed Access to Cloud Services

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

Figure 1-2 Access to cloud services

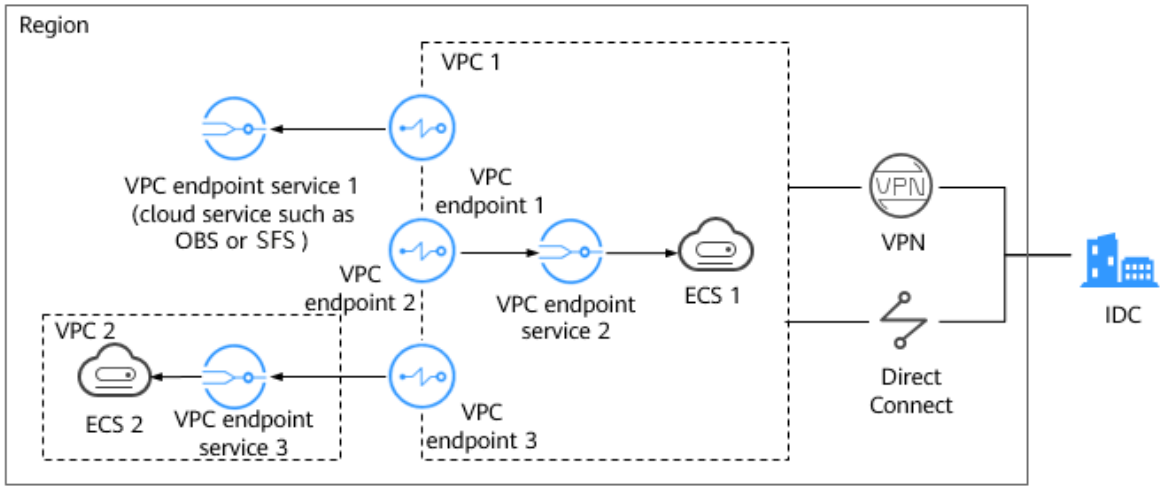


Figure 1-2 shows the process of connecting an IDC to VPC 1 over VPN or Direct Connect, for the purpose of:

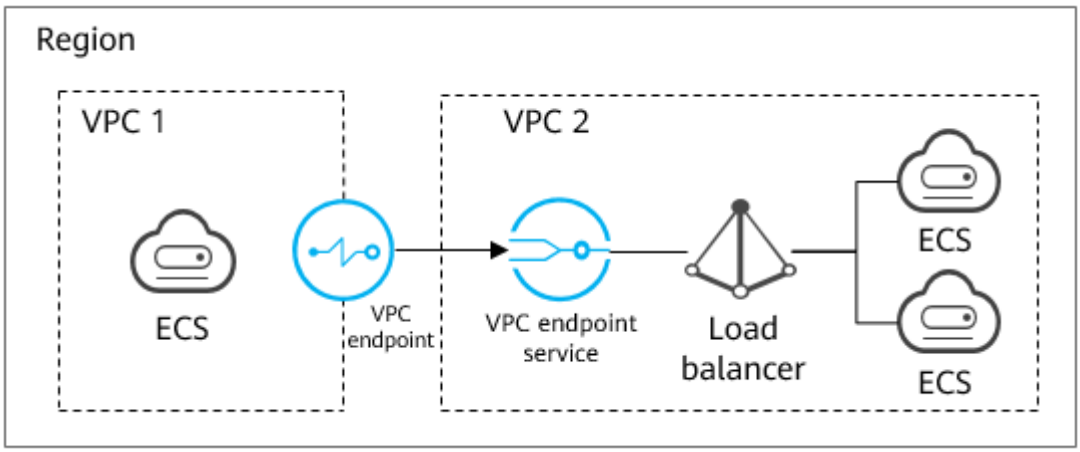
- Accessing OBS or SFS using VPC endpoint 1
- Accessing ECS 1 in the same VPC using VPC endpoint 2
- Accessing ECS 2 in VPC 2 using VPC endpoint 3

Cross-VPC Connection

With VPCEP, resources in two separate VPCs in a region can communicate with each other.

You can create an application in your VPC and configure it as a VPC endpoint service. An endpoint can be created in another VPC in the same region and then used as a channel to access the endpoint service. Figure 1-3 shows the connection details.

Figure 1-3 Cross-VPC connection



1.4 Feature List

Overview

Interface Endpoint is available to the following CPU vendors: Intel, Hygon (AMD), Kunpeng, and Phytium.

Gateway Endpoint is available to the following CPU vendors: Intel and Kunpeng.

For details about the features and functions supported by servers using different CPUs, see ***Huawei Cloud Stack 8.2.1 Infrastructure Service Feature List (Compute, Network, and Basic Management)***.

1.5 Related Services

Figure 1-4 shows the relationship between VPCEP and other cloud services.

Figure 1-4 Relationship between VPCEP and other cloud services

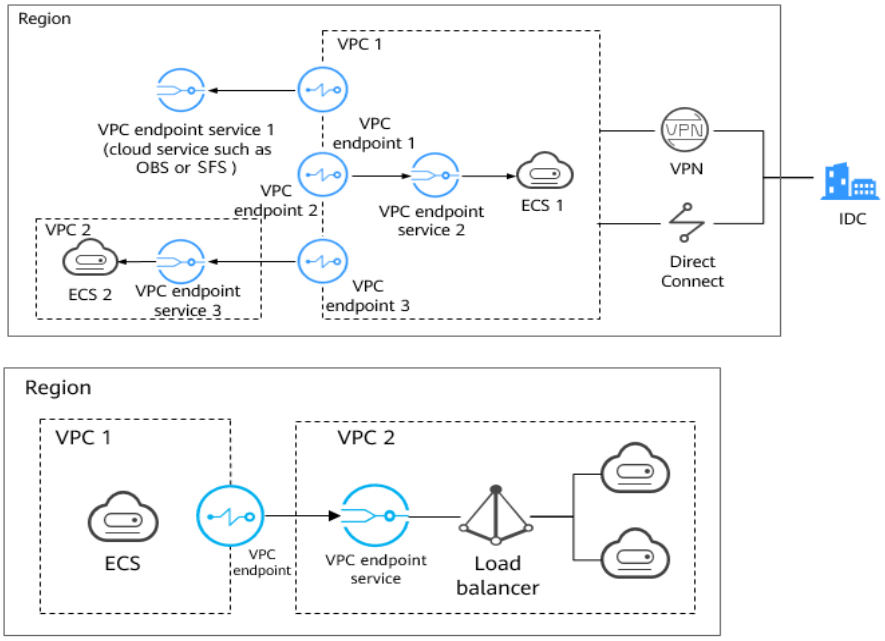


Table 1-1 VPCEP-related services

Service	Description
Virtual Private Cloud (VPC)	Two types of VPCEP resources, that is, endpoint services and endpoints, are created in two separate VPCs.
Elastic Cloud Server (ECS)	An ECS can access the ECS and ELB in another VPC through VPCEP. An ECS can also provide backend resources for endpoint services.
Elastic Load Balance (ELB)	ELB provides backend resources for endpoint services.
Object Storage Service (OBS)	You can use a VPC endpoint to access OBS.
Scalable File Service (SFS)	You can use a VPC endpoint to access SFS.

1.6 Restrictions

Before using VPCEP, learn the restrictions described in **Table 1-2**.

Table 1-2 VPCEP restrictions

Item	Restrictions
Gateway VPC endpoint	If a basic Direct Connect connection is used together with a gateway VPC endpoint to access a storage service, the CIDR block of the local subnet configured for the virtual gateway must include the CIDR block configured for the storage service, but they cannot be exactly the same.

1.7 Accessing and Using VPCEP

Two methods are available:

- Web UI

  Log in to ManageOne Operation Portal (ManageOne Tenant Portal in B2B scenarios) as a tenant, click  in the upper left corner of the page, select a region and resource set, and select the cloud service.
- API

  Use this mode if you need to integrate this service into a third-party system for secondary development. For details, see the API reference of this service on **Operation Help Center**.

2 Related Concepts

2.1 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 endpoint services are created only for cloud services.
- Interface endpoint services can be created for your private services.

Gateway Endpoint Services

Table 2-1 Supported gateway endpoint services

Endpoint Service	Category	Example	Description
Object Storage Service (OBS)	Cloud service	vpc-hz-1.a47da05c-9b1b-49cd-8e91-f9d3d8ee138c.obs	Select this endpoint service if you want to access OBS using an endpoint.
Scalable File Service (SFS)	Cloud service	vpc-hz-1.a47da05c-9b1b-49cd-8e91-f9d3d8ee138c.sfs	Select this endpoint service if you want to access SFS using an endpoint.

Interface Endpoint Services

Table 2-2 Supported interface endpoint services

Endpoint Service	Category	Example	Description
Elastic Load Balance (ELB)	Private service	None	Select a load balancer as the backend resource if your services receive high traffic and demand high reliability and disaster recovery (DR) performance.
Elastic Cloud Server (ECS)	Private service	None	ECSs can be used as servers.

2.2 Endpoints

Endpoints are created by the service user and provide a connection channel between VPCs and endpoint services. You can create an application in your VPC and configure it as an endpoint service. In the same region, you can create an endpoint in another VPC and then use this endpoint to access the endpoint service.

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

- Endpoints for accessing interface endpoint services are elastic network interfaces that have private IP addresses.
- Endpoints for accessing gateway endpoint services are gateways, with routes configured to distribute traffic to the associated gateway endpoint services. Such endpoints allow access from both inside and outside the cloud.

  To access gateway endpoint services connected to a VPC from outside the cloud, create a gateway endpoint in your VPC first and use Cloud Connect, VPN, basic Direct Connect, or enhanced Direct Connect to connect to the VPC.

2.3 VPC

The VPC service enables you to provision logically isolated, configurable, and manageable virtual networks for cloud servers, improving the security of resources in the system and simplifying network deployment. Cloud servers can be ECSs or Bare Metal Servers (BMSs).

You can specify IP address ranges, create subnets, customize security groups, and configure route tables and gateways in a VPC. This enables you to conveniently manage and configure the network and rapidly and securely modify network configurations. You can also customize access rules and network ACLs to control cloud server access within a security group and across different security groups to enhance security of cloud servers in the subnet.

2.4 Subnet

A subnet is a network segment in a VPC. Multiple subnets can be created for a VPC to manage cloud servers with different service requirements and provide cloud servers with IP address management and DNS services.

By default, cloud servers in all subnets of the same VPC can communicate with one another, while cloud servers in different VPCs cannot communicate with one another.

2.5 Security Group

A security group is a collection of access control rules for cloud servers that have the same security protection requirements and are mutually trusted in a project. The trustlist policy (Allow rules) is supported. After a security group is created, you can create different access rules for the security group to protect cloud servers in this security group.

3 Operation Process

VPCEP enables you to access resources across VPCs in a region, improving application expansion capabilities with a more connected ecosystem.

Figure 3-1 shows the VPCEP operation process.

Figure 3-1 VPCEP operation process

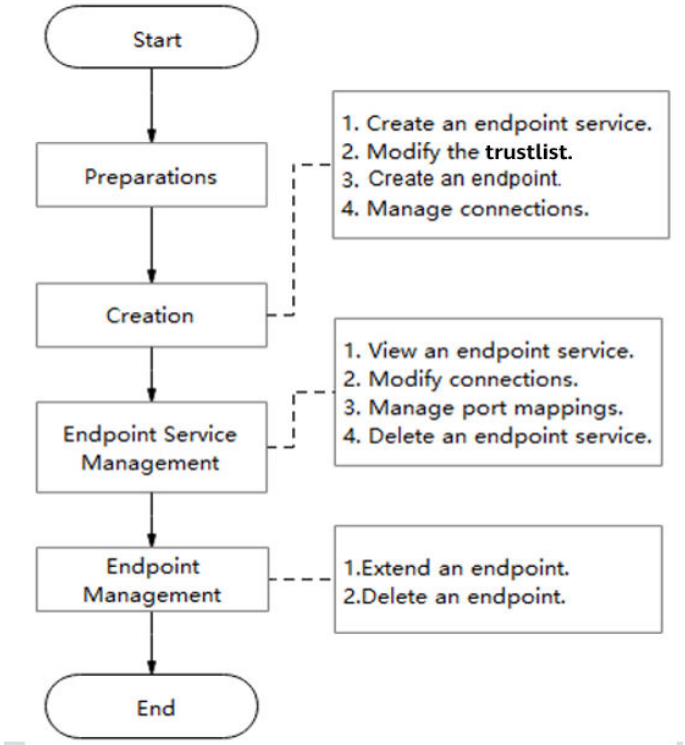


Table 3-1 Description of the VPCEP operation process

Operation	Description and Reference
Preparations	• Before using VPCEP, ensure that you obtained an account with required operation permissions. • Before using VPCEP, both the service provider and the service user must have created VPCs and subnets required for connections.
Creation	The service provider creates an endpoint service based on service requirements. For details, see **4.1 Creating an Endpoint Service**.
	After creating an endpoint service, the service provider needs to add the tenant ID of the service user to the service trustlist. For details, see **4.2 Modifying the Whitelist**.
	The service user creates an endpoint based on service requirements. For details, see **4.3 Applying for an Endpoint**.
	To connect to an endpoint service that has connection approval enabled, you need to obtain the approval of the owner of the endpoint service. For details, see **4.4 Managing Connections**.
Endpoint service management	The service provider views an endpoint service based on service requirements. For details, see **5.1 Viewing an Endpoint Service**.
	The service provider modifies connections of an endpoint service based on service requirements. For details, see **5.2 Modifying Connections**.
	The service provider manages the port mapping of an endpoint service based on service requirements. For details, see **5.3 Managing Port Mappings**.
	The service provider deletes an endpoint service based on service requirements. For details, see **5.4 Deleting an Endpoint Service**.
Endpoint management	After an endpoint expires, the service user can extend it based on service requirements. For details, see **5.5 Extending an Endpoint**.
	The service user deletes an endpoint based on service requirements. For details, see **5.6 Deleting an Endpoint**.

4 Creation

4.1 Creating an Endpoint Service

The service provider creates endpoint services to serve service users.

There are two types of VPC endpoint services:

- Gateway endpoint services are created only for cloud services.
- Interface endpoint services can be created for your private services.

Prerequisites

You have created a VPC for the endpoint to connect to and have created subnets in the VPC.

Procedure

Step 1 Log in to the VPC Endpoint console. For details, see **6.2 How Do I Log In to the VPC Endpoint Page?**

Step 2 In the navigation pane on the left of the **Network Console** page, choose **VPC Endpoint** > **VPC Endpoint Services**.

Step 3 Click **Create Endpoint Service** in the upper right of the page and set parameters as prompted. For details about the parameters, see **Table 4-1**.

Table 4-1 Parameters for creating an endpoint service

Parameter	Description
Name	This parameter is optional. Specifies the name of the endpoint service to be created. • If you do not configure this parameter, the name of the endpoint service generated by the system is in the format of *Region ID.Service ID*. • If you configure this parameter, the name of the endpoint service generated by the system is in the format of *Region ID.Name.Service ID*.
VPC	Specifies the VPC where the endpoint service is deployed.
Service Type	Specifies the type of the endpoint service. The value can only be **Interface**.
Connection Approval	Specifies whether the connection between an endpoint and an endpoint service requires approval from the owner of the endpoint service. You can determine whether to enable or disable the connection approval. If connection approval is enabled, any endpoint for connecting to the endpoint service needs to be approved. For details, see **4.4 Managing Connections**.
Port Mapping	Specifies the protocol and ports used for communication between the endpoint service and endpoint. The protocol is TCP or UDP. **Service Port**: A service port is provided by the backend service bound to the endpoint service. **Client Port**: A client port is provided by the endpoint, allowing you to access the endpoint service. The value of the service and client port number ranges from **1** to **65535**. A maximum of 50 port mappings can be added at a time.

Parameter	Description
Backend Resource Type	Specifies the type of the backend resource that provides services to be accessed. This parameter can be set to **Elastic Load Balance** or **Cloud Server**. • **Elastic Load Balance**: Backend resources of this type suit services that receive high access traffic and demand high reliability and disaster recovery (DR) performance. • **Cloud Server**: Backend resources of this type serve as servers. **NOTE** A maximum of five endpoint services can be created for a given backend resource. This parameter cannot be set to the **Elastic Load Balance** of the IPv6 type.
Elastic Load Balance	This parameter is available only when **Backend Resource Type** is set to **Elastic Load Balance**. Select the required elastic load balance service from the drop-down list.
Subnet	This parameter is available only when **Backend Resource Type** is set to **Cloud Server**. Select the required subnet from the list.
ECS	This parameter is available only when **Backend Resource Type** is set to **Cloud Server**. Select the required cloud server from the list.

Step 4 Click **Create Now** to create an endpoint service.

----End

4.2 Modifying the Whitelist

After creating an endpoint service, the service provider needs to add the tenant ID of the service user to the service whitelist. Otherwise, the endpoint service is invisible to service users.

Prerequisites

You have created a VPC for the endpoint to connect to and have created subnets in the VPC.

Procedure

Step 1 Log in to the VPC Endpoint console. For details, see **6.2 How Do I Log In to the VPC Endpoint Page?**

Step 2 In the navigation pane on the left of the **Network Console** page, choose **VPC Endpoint** > **VPC Endpoint Services**.

Step 3 Click the name of the target VPC endpoint service and then click the **Permission Management** tab.

Step 4 Configure the whitelist.

Click **Add More**, set parameters as prompted, and enter the account ID of an authorized user.

NOTE

- To allow all users to access the VPC endpoint service, enter a wildcard (*) for the authorized tenant ID parameter.
- Service users can query tenant IDs in **My Settings**. For details, see **6.6 How Do I Obtain the Tenant ID?**
- By default, a tenant has access to the endpoint service that is in the same resource set as this tenant.

Step 5 Delete one or more whitelist records.

- To delete a single record from the whitelist, locate the target authorized tenant ID and click **Delete** in the **Operation** column.
- To delete multiple records from the whitelist, select the authorized tenant IDs to be deleted and click **Delete** above the list.

----End

4.3 Applying for an Endpoint

The service user creates endpoints to connect to the created endpoint service. After applying for a VPC endpoint and connecting it to a VPC endpoint service, you can use the IP address of the VPC endpoint to access the VPC endpoint service resources.

The procedures of applying for a VPC endpoint for connecting to different types of VPC endpoint services are different.

- **Applying for an Endpoint for an Interface Endpoint Service**
- **Applying for an Endpoint for a Gateway Endpoint Service**

Prerequisites

- You have created a VPC for the endpoint to connect to and have created subnets in the VPC.
- The service provider has created an endpoint service and added the tenant ID of the service user to the service whitelist.

  NOTE

  For details about how the service provider adds the tenant ID of the service user to the service whitelist, see **4.2 Modifying the Whitelist**.

Applying for an Endpoint for an Interface Endpoint Service

Step 1 Log in to the VPC Endpoint console. For details, see **6.2 How Do I Log In to the VPC Endpoint Page?**

Step 2 In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoints**.

Step 3 On the **VPC Endpoints** page, click **Apply for Endpoint**.

Step 4 In the displayed **Select Service** dialog box, click **Apply Now**. On the displayed page, set parameters as prompted.

Table 4-2 Parameters for creating an endpoint

Parameter	Description	Example Value
Service Category	Select **Find a service by name**. **Find a service by name**: Select this option if the target VPC endpoint service is a private service of your own.	Find a service by name
Endpoint Service Name	Enter or copy a service name and click **Verify** to select a private service.	N/A
Internal Network Domain Name	This parameter is available only when the DNS service is enabled for the VPC where the endpoint service is deployed. **NOTE** If this option is selected, the system automatically creates an internal network domain name for an endpoint after the endpoint is successfully created by the service user and accepted by the service provider.	N/A
VPC	Choose a VPC for the endpoint from the drop-down list.	**vpc_ep**
Subnet	Choose a subnet for the endpoint from the drop-down list. **NOTE** The subnet for the endpoint supports only IPv4 CIDR blocks.	subnet_ep
Node IP Address	Select **Automatic** or **Manual** for assigning the private IP address of the VPC endpoint.	Automatic
Required Duration	Select the required duration for requesting an endpoint.	1 year

Step 5 Click **Apply Now**.

----End

Applying for an Endpoint for a Gateway Endpoint Service

Step 1 Log in to the VPC Endpoint console. For details, see **6.2 How Do I Log In to the VPC Endpoint Page?**

Step 2 In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoints**.

Step 3 On the **VPC Endpoints** page, click **Apply for Endpoint**.

Step 4 In the displayed **Select Service** dialog box, click **Apply Now**. On the displayed page, set parameters as prompted.

Table 4-3 Parameters for creating an endpoint

Parameter	Description	Example Value
Service Category	Select **Cloud services**. **Cloud services**: Select this option if the target VPC endpoint service is a cloud service.	Cloud services
Cloud Services	Select the required cloud service from the list. You do not have the permission to configure such endpoint services, but can select them when creating a VPC endpoint.	-
VPC	Choose a VPC for the endpoint from the drop-down list.	vpc_ep
Required Duration	Select the required duration for requesting an endpoint.	1 year

Step 5 Click **Apply Now**.

----End

4.4 Managing Connections

To connect to an endpoint service that has connection approval enabled, you need to obtain the approval of the owner of the endpoint service.

Prerequisites

- You have created a VPC for the endpoint to connect to and have created subnets in the VPC.
- The service provider has created an endpoint service.

Procedure

Step 1 Log in to the VPC Endpoint console. For details, see **6.2 How Do I Log In to the VPC Endpoint Page?**

Step 2 In the navigation pane on the left of the **Network Console** page, choose **VPC Endpoint** > **VPC Endpoint Services**.

Step 3 In the endpoint service list, locate the target endpoint service and click its name.

Step 4 Click the **Connection Management** tab.

Step 5 Accept or reject an endpoint in the list based on service requirements.

----End

5 Management

5.1 Viewing an Endpoint Service

After endpoint services are created, the service provider can select a specified endpoint service to view its basic information, connection management, permission management, and port mapping details.

Procedure

Step 1 Log in to the VPC Endpoint console. For details, see **6.2 How Do I Log In to the VPC Endpoint Page?**

Step 2 In the navigation pane on the left of the **Network Console** page, choose **VPC Endpoint** > **VPC Endpoint Services**.

Step 3 In the endpoint service list, locate the target endpoint service and click its name.

Step 4 View details of the endpoint service on the displayed page. You can also query other parameters on the **Connection Management**, **Permission Management**, and **Port Mapping** tab pages. For details, see **Table 5-1**.

Table 5-1 Parameter description

Tab	Parameter	Description
Basic Information	Name	Specifies the name of the endpoint service.
	ID	Specifies the ID of the endpoint service.
	Backend Resource Type	Specifies the type of the backend resource that provides services to be accessed. This parameter can be set to **Cloud Server** or **Elastic Load Balance**.

Tab	Parameter	Description
	Cloud Server	Specifies the name of the backend resource connected to the endpoint service. This parameter is available only when **Backend Resource Type** is set to **Cloud Server**. After the backend resource is deleted, the value of **Cloud Server** is displayed as **--**. Click **Associate** to associate the endpoint service with a cloud server again. For details, see **6.7 How Do I Resume a Suspended Endpoint Service?**
	Elastic Load Balance	Specifies the name of the backend resource connected to the endpoint service. This parameter is available only when **Backend Resource Type** is set to **Elastic Load Balance**. After the backend resource is deleted, the value of **Elastic Load Balance** is displayed as **--**. Click **Associate** to associate the endpoint service with an ELB again. For details, see **6.7 How Do I Resume a Suspended Endpoint Service?**
	VPC	Specifies the VPC where the endpoint service is deployed.
	Status	Specifies the status of the endpoint service. For details, see **6.3 What Are Statuses of Endpoint Services and Endpoints?**
	Connection Approval	Specifies whether connection approval is required.
	Service Type	Specifies the type of the endpoint service.
	NIC	Specifies the IP address of the NIC used by the cloud server. This parameter is available only when **Backend Resource Type** is set to **Cloud Server**.
	Created	Specifies the creation time of the endpoint service.
Connection Management	Endpoint ID	Specifies the ID of the endpoint.
	Packet ID	Specifies the identifier of the endpoint ID.
	Status	Specifies the status of the endpoint. For details, see **6.3 What Are Statuses of Endpoint Services and Endpoints?**
	Owner	Specifies the account ID of the user who creates the endpoint.
	Created	Specifies the creation time of the endpoint.

Tab	Parameter	Description
	Operation	Specifies whether to allow an endpoint to connect to an endpoint service. The value can be **Accept** or **Reject**.
Permission Management	Authorized Tenant ID	Specifies the ID of the authorized tenant for accessing the endpoint, or *. To allow all users to access the VPC endpoint service, enter a wildcard (*) for the authorized tenant ID parameter.
	Operation	Specifies the operation of deleting an authorized account from the whitelist.
Port Mapping	Protocol	Specifies the protocol and ports used for communication between the endpoint service and endpoint.
	Service Port	Specifies the port provided by the backend service bound to the endpoint service.
	Client Port	Specifies the port provided by the endpoint, allowing you to access the endpoint service.
	Operation	Specifies the operation of modifying or deleting a port mapping.

----End

5.2 Modifying Connections

The service provider modifies connections of an endpoint service based on service requirements.

Procedure

Step 1 Log in to the VPC Endpoint console. For details, see **6.2 How Do I Log In to the VPC Endpoint Page?**

Step 2 In the navigation pane on the left of the **Network Console** page, choose **VPC Endpoint** > **VPC Endpoint Services**.

Step 3 In the endpoint service list, locate the target endpoint service and click its name.

Step 4 Click the **Connection Management** tab.

Step 5 Accept or reject an endpoint in the list based on service requirements.

NOTE

If you change the status of a connection from **Accepted** to **Rejected**, the endpoint in the connection cannot connect to the endpoint service.

----End

5.3 Managing Port Mappings

The service provider adds, modifies, or deletes the port mapping of an endpoint service based on service requirements.

Procedure

Step 1 Log in to the VPC Endpoint console. For details, see **6.2 How Do I Log In to the VPC Endpoint Page?**

Step 2 In the navigation pane on the left of the **Network Console** page, choose **VPC Endpoint** > **VPC Endpoint Services**.

Step 3 In the endpoint service list, locate the target endpoint service and click its name.

Step 4 Click the **Port Mapping** tab to add, modify, or delete a port mapping.

Table 5-2 Operations performed to manage a port mapping

Operation	Procedure
Add a port mapping.	Click **Add Port Mapping**. On the displayed page, select a protocol, and enter the service port number and client port number.
Modify a port mapping.	Locate the target port mapping and click **Modify** in the **Operation** column. On the displayed page, modify the protocol, and enter the service port number and client port number.
Delete a port mapping.	Locate the target port mapping and click **Delete** in the **Operation** column.

----End

5.4 Deleting an Endpoint Service

The service provider deletes an endpoint service based on service requirements.

Procedure

Step 1 Log in to the VPC Endpoint console. For details, see **6.2 How Do I Log In to the VPC Endpoint Page?**

Step 2 In the navigation pane on the left of the **Network Console** page, choose **VPC Endpoint** > **VPC Endpoint Services**.

Step 3 In the endpoint service list, locate the target endpoint service and click **Delete** in the **Operation** column.

Step 4 In the displayed dialog box, click **OK**.

----End

5.5 Extending an Endpoint

After an endpoint expires, the service user can extend it based on service requirements.

Procedure

Step 1 Log in to the VPC Endpoint console. For details, see **6.2 How Do I Log In to the VPC Endpoint Page?**

Step 2 In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoints**.

Step 3 Locate the target endpoint and click **Extend** in the **Operation** column.

Step 4 In the displayed dialog box, select an extension period and click **OK**.

----End

5.6 Deleting an Endpoint

The service user deletes an endpoint based on service requirements.

Procedure

Step 1 Log in to the VPC Endpoint console. For details, see **6.2 How Do I Log In to the VPC Endpoint Page?**

Step 2 In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoints**.

Step 3 In the endpoint list, locate the target endpoint and click **Delete** in the **Operation** column.

Step 4 In the displayed dialog box, click **OK**.

----End

6 FAQs

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

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

Table 6-1 Differences between VPC endpoints and VPC peering connections

Category	VPC Endpoint	VPC Peering Connection
Security	Only the ECSs and ELBs in a VPC for which endpoint services are created can be accessed.	All the ECSs and load balancers in a VPC subnet to which a peering connection route is added can be accessed by the peer VPC.
CIDR overlap	Supported If you use a VPC endpoint to connect two VPCs, you do not have to worry about overlapping subnets.	Not supported If two VPCs have overlapping subnets, the VPC peering connection created between the two VPCs cannot work, so the two VPCs cannot communicate with each other.
Communication mode	For two VPCs connected by a VPC endpoint, only the VPC with the VPC endpoint deployed can initiate an access request to the other VPC with the endpoint service deployed through a specified port.	Bidirectional communication is supported for two VPCs between which a VPC peering connection is created.

Category	VPC Endpoint	VPC Peering Connection
Route configuration	For two VPCs that are connected through a VPC endpoint, the route has been configured, and you do not need to configure it again.	If a peering connection is established between two VPCs, you need to add the connection route to the VPCs, so that they can communicate with each other.

6.2 How Do I Log In to the VPC Endpoint Page?

Step 1 Log in to ManageOne as a VDC administrator or VDC operator using a browser.

URL in non-B2B scenarios: **https://***Domain name of ManageOne Operation Portal*, for example, **https://console.demo.com**.

URL in B2B scenarios: **https://***Domain name of ManageOne Tenant Portal*, for example, **https://tenant.demo.com**.

URL of the unified portal: **https://***Domain name of the ManageOne unified portal*, for example, **https://console.demo.com/moserviceaccesswebsite/unifyportal#/home**. On the homepage, choose **Self-service Cloud Service Center** to go to ManageOne Operation Portal.

You can log in using a password or a USB key.

- Login using a password: Enter the username and password.

  The password is that of the VDC administrator or VDC operator.
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

Step 2 Click  on the left of the main menu, select a region and resource set, and choose **Network** > **VPC Endpoint**.

----End

6.3 What Are Statuses of Endpoint Services and Endpoints?

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

Table 6-2 Statuses of an endpoint service

Status	Description
Creating	Indicates that the endpoint service is being created.
Connectable	Indicates that the endpoint service is created and can accept an endpoint.

Status	Description
Failed	Indicates that the endpoint service fails to be created.
Suspended	Indicates that the backend resource is deleted after the endpoint service is created.
Deleting	Indicates that the endpoint service is being deleted.
Deleted	Indicates that the endpoint service has been deleted.

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

Table 6-3 Statuses of an endpoint

Status	Description
Creating	Indicates that the endpoint is connecting to the associated endpoint service.
Awaiting acceptance	Indicates that the endpoint is pending acceptance of the owner of the associated endpoint service.
Accepted	Indicates that the endpoint is accepted by the associated endpoint service.
Rejected	Indicates that the endpoint is rejected by the associated endpoint service.
Failed	Indicates that the endpoint fails to connect to the associated endpoint service.
Deleting	Indicates that the endpoint is being deleted.

6.4 Can a VPC with an Endpoint Service Be Deleted?

A VPC where an endpoint service is deployed cannot be deleted. You must delete the endpoint service before deleting the VPC.

6.5 What Do I Do If the Endpoint Service Is Unavailable When I Am Creating an Endpoint?

If the tenant ID of a service user is not added to the whitelist of the endpoint service, the endpoint service is unavailable for the service user.

Contact the service provider to add the tenant ID to the whitelist. For details, see **4.2 Modifying the Whitelist**.

6.6 How Do I Obtain the Tenant ID?

The service provider needs to enter the tenant ID of the service user when configuring the trustlist. The tenant ID is provided by the service user.

Procedure

Step 1 Log in to ManageOne as a VDC administrator or VDC operator using a browser.

URL in non-B2B scenarios: **https://***Domain name of ManageOne Operation Portal*, for example, **https://console.demo.com**.

URL in B2B scenarios: **https://***Domain name of ManageOne Tenant Portal*, for example, **https://tenant.demo.com**.

URL of the unified portal: **https://***Domain name of the ManageOne unified portal*, for example, **https://console.demo.com/moserviceaccesswebsite/unifyportal#/home**. On the homepage, choose **Self-service Cloud Service Center** to go to ManageOne Operation Portal.

You can log in using a password or a USB key.

- Login using a password: Enter the username and password.

  The password is that of the VDC administrator or VDC operator.
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter a PIN.

Step 2 Move your cursor to the tenant avatar in the upper right corner of the navigation bar and click **My Settings** on the menu that is displayed to obtain the tenant ID.

----End

6.7 How Do I Resume a Suspended Endpoint Service?

If a backend resource associated with the endpoint service is deleted or the endpoint service cannot be associated with a backend resource due to NIC modification, the endpoint service is still retained and its status changes to **Suspended**. The service provider can associate the suspended endpoint service with a backend resource again to resume the endpoint service.

Procedure

Step 1 Log in to the VPC Endpoint console. For details, see **6.2 How Do I Log In to the VPC Endpoint Page?**

Step 2 In the navigation pane on the left of the **Network Console** page, choose **VPC Endpoint** > **VPC Endpoint Services**.

Step 3 Click the endpoint service in the **Suspended** state to view its basic information.

Step 4 After the backend resource is deleted, the value of **Cloud Server** or **Elastic Load Balance** is displayed as **--**. Click **Associate** to associate the endpoint service with a backend resource again.

NOTE

The type of the new backend resource must be the same as the original one. If the backend resource type is **Cloud Server**, associate the endpoint service with the required cloud server and select a NIC. If the backend resource type is **Elastic Load Balance**, associate the endpoint service with the required elastic load balance service.

----End

