

# VPC Endpoint

# Best Practices

**Issue** 01  
**Date** 2022-09-30



**Copyright © Huawei Technologies Co., Ltd. 2023. All rights reserved.**

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

## **Trademarks and Permissions**



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

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

## **Notice**

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

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

---

# Contents

---

<b>1 Using VPCEP and Direct Connect to Enable On-premises Data Centers to Access Cloud Services.....</b>	<b>1</b>
1.1 Overview.....	1
1.2 Resource and Cost Planning.....	3
1.3 On-premises Data Center Accessing Cloud Resources Through Huawei Cloud Intranet.....	4
1.4 Procedure.....	5

# 1 Using VPCEP and Direct Connect to Enable On-premises Data Centers to Access Cloud Services

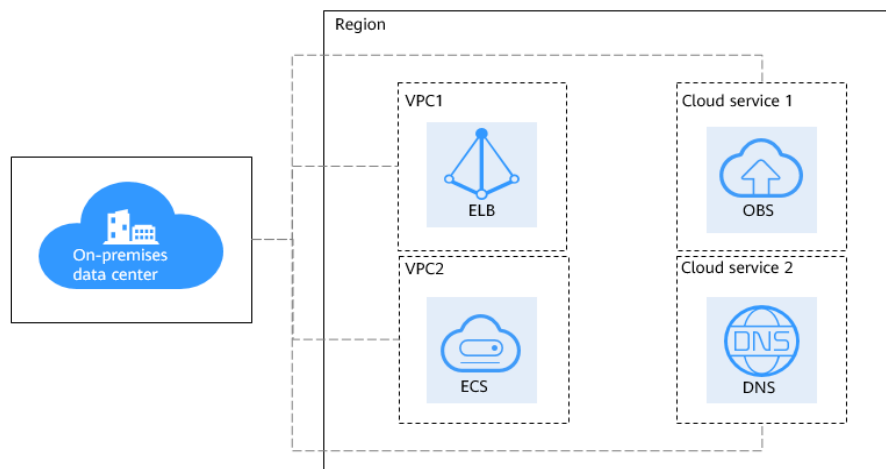
---

## 1.1 Overview

### Scenarios

After enterprise A migrated some of its workloads to the cloud through Direct Connect or VPN, its on-premises data center maintains a complex hybrid cloud architecture for a long time. Some production and testing workloads are running on on-premises data centers, and some production and testing workloads are running on Huawei Cloud or other cloud platforms. In this way, the on-premises data center often needs to access cloud services through intranets. However, many cloud resources and services still cannot be accessed through Direct Connect or VPN only.

As shown in [Figure 1-1](#), the on-premises data center prefers to access ELB in VPC1, ECS in VPC2, and other cloud services (OBS and DNS) without using the Internet.

**Figure 1-1** On-premises data center accessing Huawei cloud services

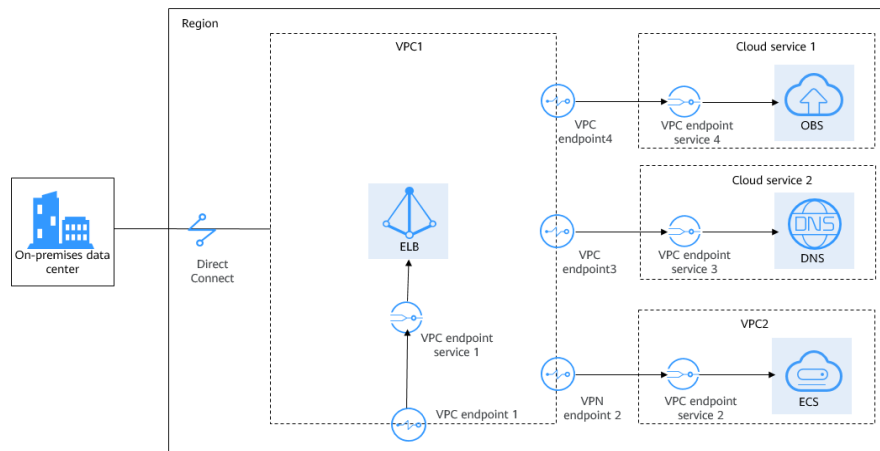
## Solution Architecture

To meet enterprise A's requirements of communicating with Huawei Cloud and accessing resources and other cloud services in VPCs without using the public network, we offer the customer a solution in which the following two services are used:

- **Direct Connect:** a service that allows enterprise A to establish a stable, high-speed, low-latency, secure dedicated connection that connects A's on-premises data center to Huawei Cloud. Direct Connect allows A to maximize legacy IT facilities and leverage cloud services to build a flexible, scalable hybrid cloud computing environment.
- **VPC Endpoint:** VPCEP enables A to access Huawei Cloud services or other private services over the Huawei Cloud network. It provides flexible networking without having to use EIPs.

As shown in **Figure 1-2**:

- Direct Connect enables communications between A's on-premises data center and VPC1.
- With VPC endpoint 1, enterprise A accesses ELB in VPC1 from its on-premises data center.
- With VPC endpoint 2, enterprise A accesses ECSs in VPC2.
- With VPC endpoint 3, enterprise A accesses Domain Name Service (DNS) over the intranet.
- With VPC endpoint 4, enterprise A accesses Object Storage Service (OBS) over the intranet.

**Figure 1-2** On-premises data center accessing Huawei Cloud services with Direct Connect and VPCEP**CAUTION**

Not all cloud services can be accessed from on-premises data center through VPC endpoints over the intranet. Only services that support VPCEP can access cloud resources and services over the intranet.

## Advantages

- VPC endpoints take effect a few seconds after they are created.
- Customers can use VPC endpoints to access cloud resources across VPCs without having to use EIPs.
- Unknown risks caused by server information leakage can be prevented, ensuring security and privacy.

## Constraints and Limitations

- You have a Huawei Cloud account, and the Huawei Cloud account has been configured with operation permissions of related services.
- The account is not in arrears and the account balance is sufficient to pay for the resources involved in this best practice.
- Direct Connect locations have been determined and the site survey of on-premises data centers have been completed together with the carrier. For details, see [Preparations](#).
- The cloud resources or services that users need to access have been developed based on the VPCEP standard development process and rolled out in the corresponding region.

## 1.2 Resource and Cost Planning

The following table describes the resource planning in the best practice.

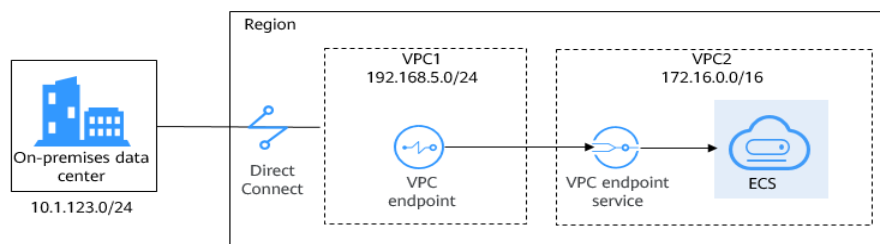
**Table 1-1** Description for cross-region VPC communication

Region	Resource	Description	Quantity	Billing
EU-Dublin	VPC	Subnet of VPC1: 192.168.0.0/16 Subnet of VPC2: 172.16.0.0/16	2	Free
	Connection	<ul style="list-style-type: none"> <li>Local subnet of the virtual gateway: 192.168.5.0/24</li> <li>Local gateway of the virtual interface: 10.0.0.1/30</li> <li>Remote gateway of the virtual interface: 10.0.0.2/30</li> <li>Remote subnet of the virtual interface: 10.1.123.0/24</li> </ul>	1	For details, see Direct Connect <a href="#">Product Pricing Details</a> .
	ECS	The IP address is automatically assigned.	2	For details, see ECS <a href="#">Product Pricing Details</a> .
	VPC endpoint	The IP address is automatically assigned.	1	For details, see VPCEP <a href="#">Product Pricing Details</a> .

The network topology is as follows.

- The on-premises data center is connected to VPC1 through Direct Connect.
- VPC1 accesses the ECS in VPC2 through the VPC endpoint service.
- The on-premises data center accesses the ECS in VPC2 through VPC1.

**Figure 1-3** Network topology



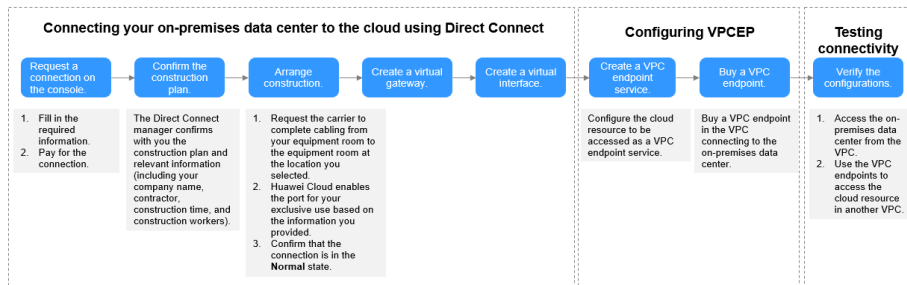
## 1.3 On-premises Data Center Accessing Cloud Resources Through Huawei Cloud Intranet

This practice describes how to access cloud servers in a VPC from an on-premises data center.

Enterprise A's on-premises data center is connected to a VPC through a Direct Connect connection and needs to access cloud servers in the VPC without using the public network.

Figure 1-4 shows the operation process of this best practice.

Figure 1-4 Process of using Direct Connect and VPCEP to access cloud resources



## 1.4 Procedure

### Step 1 Create a Direct Connect connection.



1. Create a connection.
  - a. Log in to the management console.
  - b. On the console homepage, click  in the upper left corner and select the desired region and project.
  - c. Hover on  to display **Service List** and choose **Networking > Direct Connect**.
  - d. In the navigation pane on the left, choose **Direct Connect > Connections**.
  - e. Click **Create Connection**.
  - f. On the **Create Connection** page, enter the equipment room details and select the Direct Connect location and port based on [Table 1-2](#).

Table 1-2 Parameters required for creating a connection

Parameter	Description
Billing Mode	Specifies how you are charged for the connection. Only <b>Yearly/ Monthly</b> is supported.
Region	Specifies the region where the connection is deployed. You can change the region in the upper left corner of the console.
Connection Name	Specifies the name of your connection.



Parameter	Description
Location	Specifies the location where your leased line can connect to.
Carrier	Specifies the carrier that provides the leased line.
Port Type	Specifies the type of the port that the leased line is connected to. There are four types of ports: 1GE, 10GE, 40GE, and 100GE.
Leased Line Bandwidth	Specifies the bandwidth of the leased line in the unit of Mbit/s. This is the bandwidth of the leased line you bought from the carrier.
Your Equipment Room Address	Specifies the address of your equipment room. The address must be specific to the floor your equipment room is on, for example, <i>XX</i> Equipment Room, <i>XX</i> Building, No. <i>XX</i> , Huajing Road, Pudong District, Shanghai.
Tags	Identifies the connection. A tag consists of a key and a value. You can add 10 tags to a connection. Tag keys and values must meet requirements listed in <a href="#">Table 1-3</a> . <b>NOTE</b> If a predefined tag has been created on TMS, you can directly select the corresponding tag key and value. For details about predefined tags, see <a href="#">Predefined Tag Overview</a> .
Description	Provides supplementary information about the connection.
Contact Person/Phone Number/Email	Specifies who is responsible for your connection. <b>CAUTION</b> If you do not provide any contact information in this field, we will contact the person in your account information.
Required Duration	Specifies how long the connection will be used for.

Parameter	Description
Auto-renew	Specifies whether to automatically renew the subscription to ensure service continuity.  For example, if the required duration is three months, the system automatically renews the subscription for another three months.
Enterprise Project	Provides a cloud resource management mode where cloud resources and members are centrally managed by project.



**Table 1-3** Tag key and value requirements

Parameter	Requirement
Key	<ul style="list-style-type: none"><li>▪ Cannot be left blank.</li><li>▪ Must be unique for each resource.</li><li>▪ Can contain a maximum of 36 Unicode characters.</li><li>▪ Can contain only letters, digits, hyphens, and underscores.</li></ul>
Value	<ul style="list-style-type: none"><li>▪ Can be left blank.</li><li>▪ Can contain a maximum of 43 Unicode characters.</li><li>▪ Can contain only letters, digits, period, hyphens, and underscores.</li></ul>

- g. Click **Confirm Configuration**.
        - h. Confirm the connection information and click **Pay Now**.
        - i. Confirm the order, select a payment method, and click **Confirm**.
2. Connect your on-premises data center to the cloud.
  - a. After you have paid for the order, the system automatically allocates a connection ID for you, and the connection information is displayed on the management console. The connection status is **Creating**, when you will be contacted to confirm the construction plan and relevant information (including your company name, constructor, expected construction time, and construction workers).
  - b. After having confirmed the construction plan, you can arrange the carrier to deploy the dedicated line and connect it to your equipment room based on your construction plan.

- c. In normal cases, Huawei resident engineers will connect the dedicated line to the Huawei Cloud gateway port within two working days.
  - d. After the construction is complete, the connection status becomes Normal, indicating that the connection is ready.
3. Create a virtual gateway.
    - a. In the navigation pane on the left, choose **Direct Connect > Virtual Gateways**.
    - b. Click **Create Virtual Gateway**.
    - c. Configure the virtual gateway parameters.
    - d. Click **OK**.
  4. Create a virtual interface.
    - a. In the navigation pane on the left, choose **Direct Connect > Virtual Interfaces**.
    - b. Click **Create Virtual Interface**.
    - c. Configure the virtual interface parameters.
    - d. Click **Create Now**.

## Step 2 Create a VPC endpoint service.

1. Log in to the management console.
2. On the console homepage, click  in the upper left corner and select the desired region and project.
3. Hover on  to display **Service List** and choose **Networking > VPC Endpoint**.
4. In the navigation pane on the left, choose **VPC Endpoint > VPC Endpoint Services**.
5. On the displayed page, click **Create VPC Endpoint Service**.
6. Configure the parameters.
7. Click **Create Now**.

### NOTE

In this practice, **Connection Approval** is enabled when you create a VPC endpoint service. You need to accept the connection from your purchased VPC endpoint.

## Step 3 Buy a VPC endpoint.

1. In the navigation pane on the left, choose **VPC Endpoint > VPC Endpoints**.
2. On the displayed page, click **Buy VPC Endpoint**.
3. Configure the parameters.
4. Click **Next**.
5. Confirm the order details and click **Submit**.
6. Approve the connection.

**Connection Approval** is enabled in [Step 2](#). If the VPC endpoint status is **Pending acceptance**, perform the following operations to approve connection to the VPC endpoint service:

- a. In the navigation pane on the left, choose **VPC Endpoint > VPC Endpoint Services**.
- b. In the VPC endpoint service list, locate the target VPC endpoint service and click its name.
- c. On the displayed page, select the **Connection Management** tab.
- d. In the **Operation** column, click **Accept**.

#### Step 4 (Optional) Verify the connectivity.

- ECS1 in VPC1 can access the on-premises data center (10.1.123.1).

```
Authorized users only. All activities may be monitored and reported.
ecs1 login: root
Password:
Last login: Wed Nov 10 16:24:52 on tty1

      Welcome to Huawei Cloud Service

[root@ecs1 ~]# ping 10.1.123.1
PING 10.1.123.1 (10.1.123.1) 56(84) bytes of data:
64 bytes from 10.1.123.1: icmp_seq=1 ttl=255 time=255 ms
64 bytes from 10.1.123.1: icmp_seq=2 ttl=255 time=5.41 ms
64 bytes from 10.1.123.1: icmp_seq=3 ttl=255 time=5.27 ms
64 bytes from 10.1.123.1: icmp_seq=4 ttl=255 time=5.42 ms
64 bytes from 10.1.123.1: icmp_seq=5 ttl=255 time=5.70 ms
^C
--- 10.1.123.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 5.274/55.320/254.793/99.736 ms
[root@ecs1 ~]#
```

- The VPC endpoint can access ECS2 in VPC2.

```
Authorized users only. All activities may be monitored and reported.
ecs1 login: root
Password:
Last login: Wed Nov 10 15:04:33 on tty1

      Welcome to Huawei Cloud Service

[root@ecs1 ~]# ssh 192.168.5.111
The authenticity of host '192.168.5.111 (192.168.5.111)' can't be established.
ED25519 key fingerprint is SHA256:X3pUwri0B/u0BUHJ0EZwPggjIz+uEoa7USf6Ix/nH4g.
No matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.5.111' (ED25519) to the list of known hosts.

Authorized users only. All activities may be monitored and reported.
root@192.168.5.111's password:

      Welcome to Huawei Cloud Service

Last login: Wed Nov 10 14:54:59 2021 from 198.19.131.4
[root@ecs2 ~]#
```

----End