VPC Endpoint

Best Practices

Issue 01

Date 2024-05-30

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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.

Contents

1 Using VPC Endpoint and Direct Connect to Enable On-premises Data Centers to Access Cloud Services

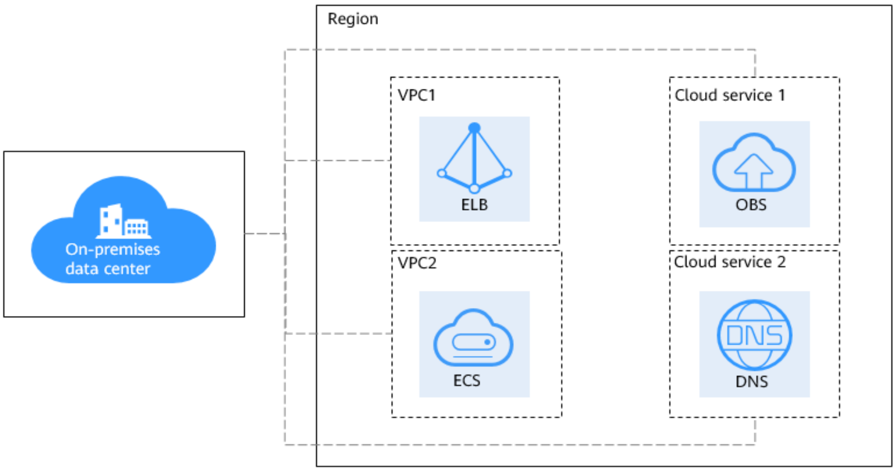
1.1 Overview

Scenarios

After an enterprise migrated some of its workloads to the cloud through Direct Connect or VPN, some production and testing workloads are running in its on-premises data center, and some are running on Huawei Cloud or other cloud platforms. With such a complex hybrid cloud architecture, 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 Virtual Private Network (VPN) only.

Figure 1-1 shows the enterprise's requirements: The on-premises data center accesses 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

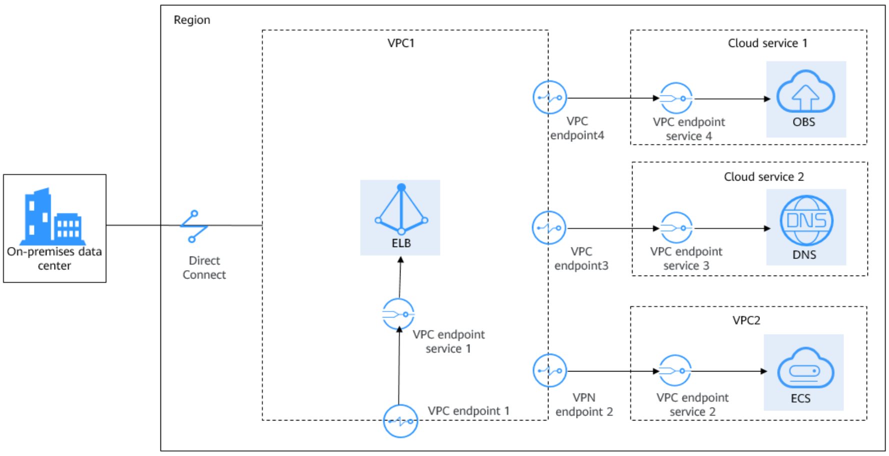
In the solution we offered to meet their requirements, the following two services are used:

- **Direct Connect**: a service that was used to establish a stable, high-speed, low-latency, secure dedicated connection between the on-premises data center and Huawei Cloud. With Direct Connect, the enterprise maximized legacy IT facilities and built a flexible, scalable hybrid cloud computing environment.
- **VPC Endpoint**: VPC Endpoint enables access to Huawei Cloud services or other private services over the Huawei Cloud network. It provides flexible networking, freeing the enterprise from using EIPs.

In **Figure 1-2**,

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

Figure 1-2 On-premises data center accessing Huawei Cloud services with Direct Connect and VPC Endpoint



⚠ CAUTION

Not all cloud services can be accessed from an on-premises data center through VPC endpoints over the intranet. Only services that support VPC Endpoint 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 resources across VPCs without having to use EIPs.
- Unknown risks caused by server information leakage can be prevented, ensuring security and privacy.

Constraints

- A HUAWEI ID is available and must be configured with operation permissions for related services.
- The HUAWEI ID is not in arrears and the balance is sufficient to pay for the resources involved in this best practice.
- Direct Connect locations have been determined and the site survey of the on-premises data center has been completed together with the carrier. For details, see **Preparations**.
- The cloud resources or services to be accessed have been developed based on the VPC Endpoint 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.

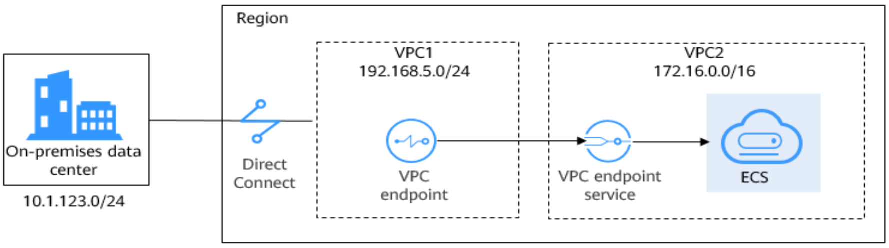
Table 1-1 Description for cross-region VPC communications

Region	Resource	Description	Quantity	Billing
CN-Hong Kong	VPC	Subnet of VPC1: 192.168.0.0/16 Subnet of VPC2: 172.16.0.0/16	2	Free
	Connection	● Local subnet of the virtual gateway: 192.168.5.0/24 ● Local gateway of the virtual interface: 10.0.0.1/30 ● Remote gateway of the virtual interface: 10.0.0.2/30 ● Remote subnet of the virtual interface: 10.1.123.0/24	1	For details, see Direct Connect **Product Pricing Details**.
	ECS	The IP address is automatically assigned.	2	For details, see ECS **Product Pricing Details**.
	VPC endpoint	The IP address is automatically assigned.	1	For details, see VPC Endpoint **Product Pricing Details**.

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



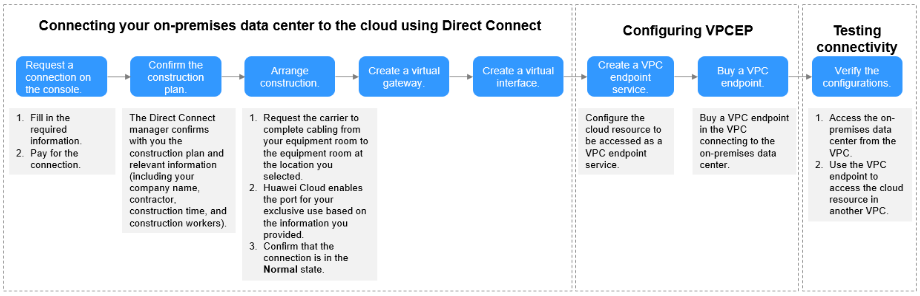
1.3 On-premises Data Center Accessing Cloud Resources Through the Huawei Cloud Intranet

This practice is about accessing cloud servers in a VPC from an on-premises data center.

The 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 Internet.

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

Figure 1-4 Process for using Direct Connect and VPC Endpoint to access cloud resources


Connecting your on-premises data center to the cloud using Direct Connect
Request a connection on the console.
Confirm the construction plan.
Arrange construction.
Create a virtual gateway.
Create a virtual interface.
Configuring VPCEP
Create a VPC endpoint service.
Buy a VPC endpoint.
Testing connectivity
Verify the configurations.

1. Fill in the required information.
2. Pay for the connection.

The Direct Connect manager confirms with you the construction plan and relevant information (including your company name, contractor, construction time, and construction workers).

1. Request the carrier to complete cabling from your equipment room to the equipment room at the location you selected.
2. Huawei Cloud enables the port for your exclusive use based on the information you provided.
3. Confirm that the connection is in the **Normal** state.

Configure the cloud resource to be accessed as a VPC endpoint service.

Buy a VPC endpoint in the VPC connecting to the on-premises data center.

1. Access the on-premises data center from the VPC.
2. Use the VPC endpoint to access the cloud resource in another VPC.

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**.

      The **Connections** page is displayed.
   d. Click **Create Connection**.
   e. 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 **Yearly/ Monthly** 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.
Tag	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 **Table 1-3**. **NOTE** If a predefined tag has been created on Tag Management Service (TMS), you can directly select the corresponding tag key and value. For details about predefined tags, see **Predefined Tag Overview**. If you have configured tag policies for Direct Connect, you need to add tags to your connections based on the tag policies. If you add a tag that does not comply with the tag policies, connections may fail to be created. Contact the administrator to learn more about tag policies.
Description	Provides supplementary information about the connection.
Contact Person/Phone Number/ Email	Specifies who is responsible for your connection.
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 and you have selected **Auto-renew**, the system automatically renews the subscription for another three months.
Enterprise Project	Centrally manages cloud resources and members by project.

Table 1-3 Tag key and value requirements

Parameter	Requirement
Key	▪ Cannot be left blank. ▪ Must be unique for each resource. ▪ Can contain a maximum of 36 characters. ▪ Can contain only letters, digits, hyphens (-), and underscores (_).
Value	▪ Can be left blank. ▪ Can contain a maximum of 43 characters. ▪ Can contain only letters, digits, period, hyphens (-), and underscores (_).

f. Click **Confirm Configuration**.

g. Confirm the connection information and click **Pay Now**.

h. 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. Hover on ☰ to display **Service List** and choose **Networking** > **VPC Endpoint**.
2. In the navigation pane on the left, choose **VPC Endpoint** > **VPC Endpoint Services**.
3. On the displayed page, click **Create VPC Endpoint Service**.
4. Configure the parameters.
5. 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.

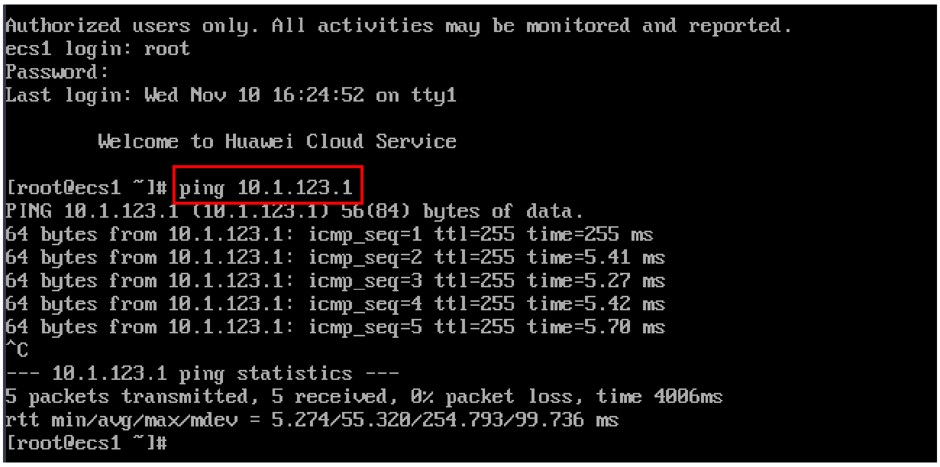
   Connection Approval is enabled in **Step 2**. If the VPC endpoint status is **Pending acceptance**, perform the following operations to approve the connection to the VPC endpoint service:

   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.

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).

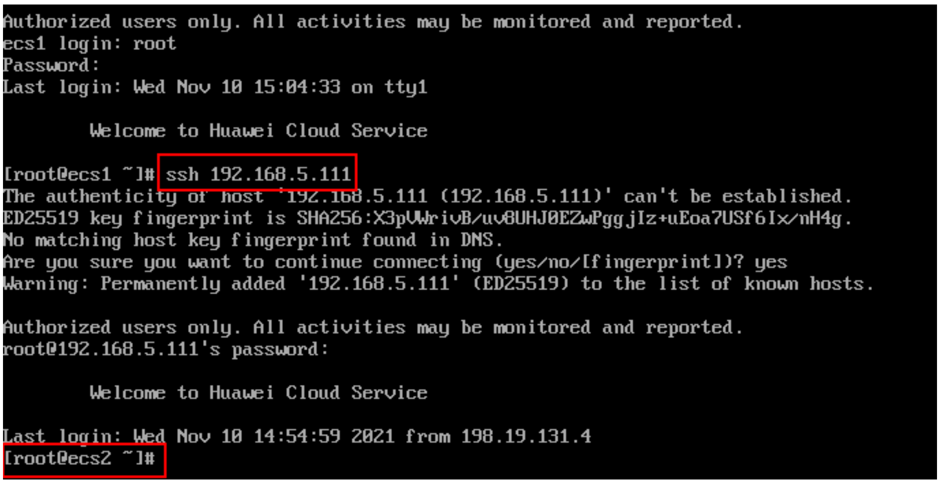


```
Authorized users only. All activities may be monitored and reported.
ecs1 login: root
Password:
Last login: Wed Nov 10 16:24:52 on tty1

        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:X3pVWrivB/uv8UHJ0EZwPggjIz+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