

Direct Connect

Service Overview

Issue 01
Date 2024-10-23



Copyright © Huawei Cloud Computing 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 Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI 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

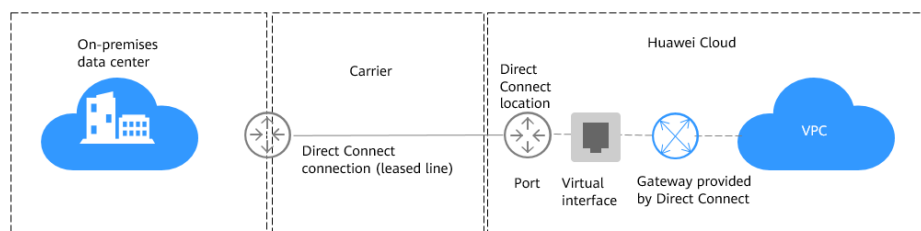
1 What Is Direct Connect?	1
2 Product Advantages	3
3 Application Scenarios	4
4 Network Planning	6
5 Notes and Constraints	9
6 Direct Connect Locations	11
7 Billing	12
8 Permissions	15
9 Direct Connect and Other Services	19
10 Basic Concepts	21
10.1 Connection	21
10.2 Virtual Gateway	22
10.3 Virtual Interface	22
10.4 Region and AZ	22

1 What Is Direct Connect?

Direct Connect allows you to establish a stable, high-speed, low-latency, secure dedicated network connection that connects your on-premises data center to Huawei Cloud. Direct Connect allows you to maximize legacy IT facilities and leverage cloud services to build a flexible, scalable hybrid cloud computing environment.

Figure 1-1 shows how Direct Connect connects an on-premises data center to the cloud.

Figure 1-1 How Direct Connect works



Why Direct Connect?

- **Network quality:** Direct Connect allows you to establish a dedicated network for data transmission, which brings high network performance, low latency, and excellent user experience.
- **Security:** Direct Connect establishes private connectivity between your on-premises data center and the cloud. Data is transmitted over a secure dedicated connection.
- **Transmission speed:** A single connection supports up to 100 Gbit/s of bandwidth.

Components

The key components of Direct Connect are a connection, virtual gateway, and virtual interface.

- **Connection**
A dedicated network connection is established between your on-premises data center and a Direct Connect location over a line you leased from a

carrier. You can create a standard connection by yourself or request a hosted connection from a partner. After you are certified as a partner, you can also create an operations connection.

A standard or operations connection has a dedicated port for your exclusive use and can be associated with multiple virtual interfaces.

A hosted connection allows you to share a port. Partners with operations connections can provision hosted connections and allocate VLANs and bandwidths for those connections. You can request hosted connections from these partners, and only one virtual interface can be created for a hosted connection.

- Virtual gateway

A virtual gateway is a logical gateway for accessing VPCs. A virtual gateway can be associated with only one VPC, and multiple connections can use the same virtual gateway to access one VPC.

- Virtual interface

A virtual interface links a connection with one or more virtual gateways, each of which is associated with a VPC, so that your on-premises network can access all these VPCs.

Accessing Direct Connect

The public cloud provides a web-based user interface, the management console, for you to access the Direct Connect service.

2 Product Advantages

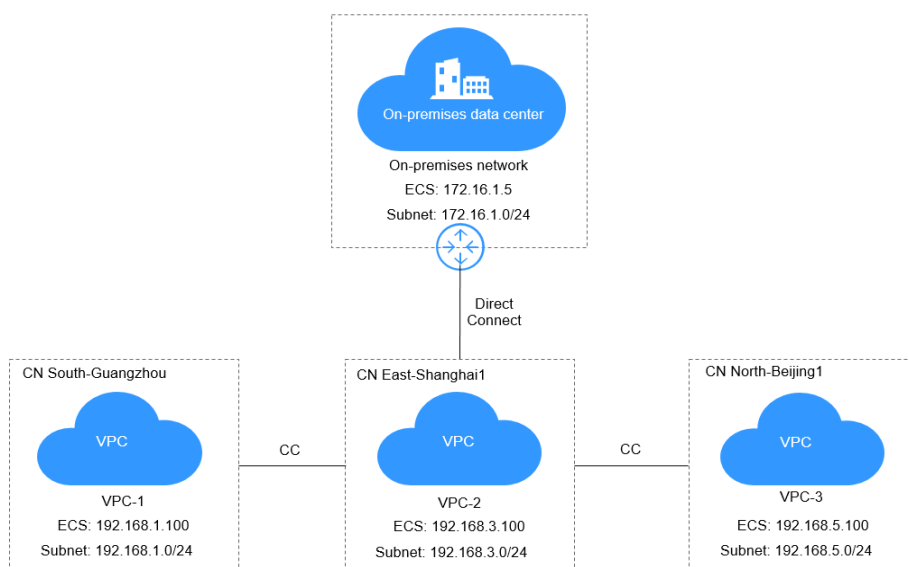
Direct Connect has the following advantages:

- **Dedicated Channels to Safeguard Data Security**
 - Establish private connectivity between your on-premises network and the cloud for stable data transmission without compromising privacy.
 - Secure your data using encrypted, dedicated connections, which provide higher security and more reliability.
- **Multiple Access Options**
 - You can select from optical bare fibers and other types of leased lines, such as MSTP and MPLS VPN.
 - There are a number of Direct Connect locations around the globe, so you can access the cloud from anywhere nearby.
- **Great Scalability for Flexible Service Deployment**
 - By building a hybrid cloud, you can gain access to virtually unlimited cloud resources for flexible, scalable deployment.
 - You can run workloads that span on-premises infrastructure and different cloud regions and flexibly connect networks across regions.
- **Ultra-low Latency and Stable Transmission**
 - Enjoy faster speeds with up to 100 Gbit/s of bandwidth, which meets the requirements of a wide range of services.
 - Configure your connections in active/active or active/standby pairs for higher reliability.

3 Application Scenarios

Access to Multiple VPCs from an On-premises Data Center

After you connect your on-premises data center to the cloud using Direct Connect, you can use Cloud Connect to connect the VPC that your on-premises data center is accessing to those in other regions, so that your on-premises data center can access all connected VPCs.



Hybrid Cloud Deployment

Direct Connect allows you to build a hybrid environment for your on-premises data center and leverage the scalability of the cloud to expand the computing capability of your applications.

Figure 3-1 Hybrid cloud

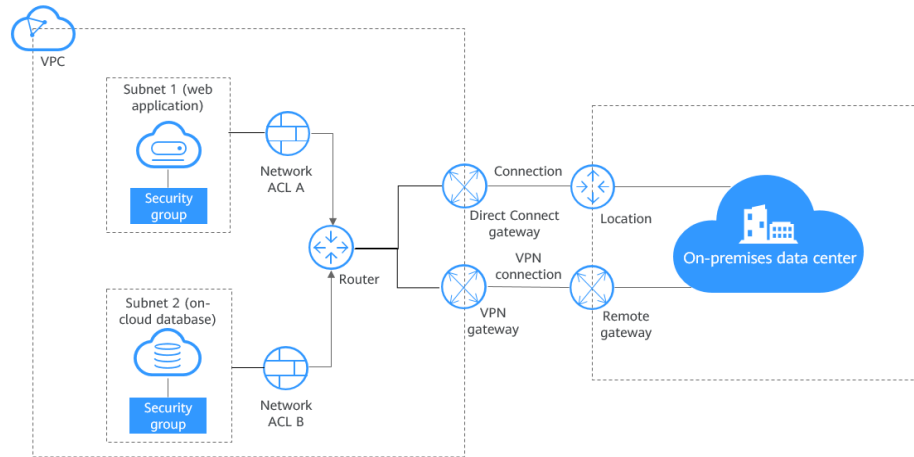


Table 3-1 Comparisons of Direct Connect and VPN in hybrid cloud deployment

Cloud Service	Scenario	Description
Virtual Private Network (VPN)	Connect an on-premises data center to the cloud through an IPsec tunnel.	VPN uses an encrypted communications tunnel to connect a VPC on the cloud to an on-premises data center and sends traffic over the Internet. It is inexpensive, easy to configure, and easy to use. However, VPN connections may be affected by the Internet quality.
Direct Connect	Connect an on-premises data center to the cloud using a dedicated network connection.	Direct Connect provides physical connections between VPCs and data centers. It has the advantages of low latency and is very secure. Direct Connect is a good choice when there are strict requirements on network transmission quality.

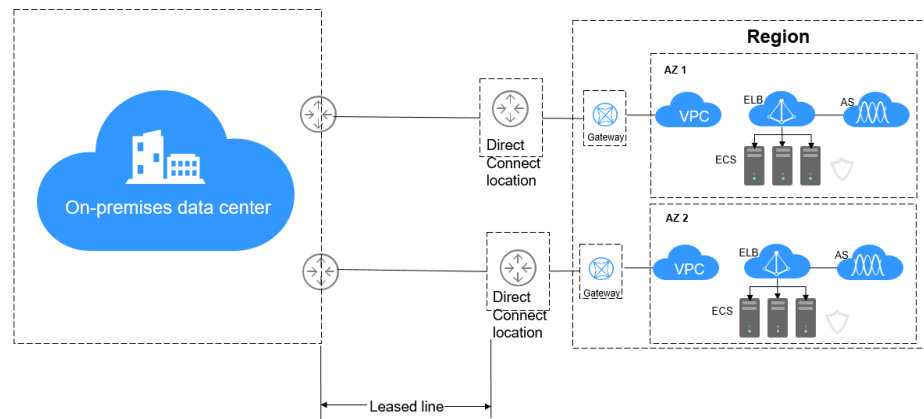
4 Network Planning

Overview

You can connect your on-premises data center to the cloud using a standard or hosted connection:

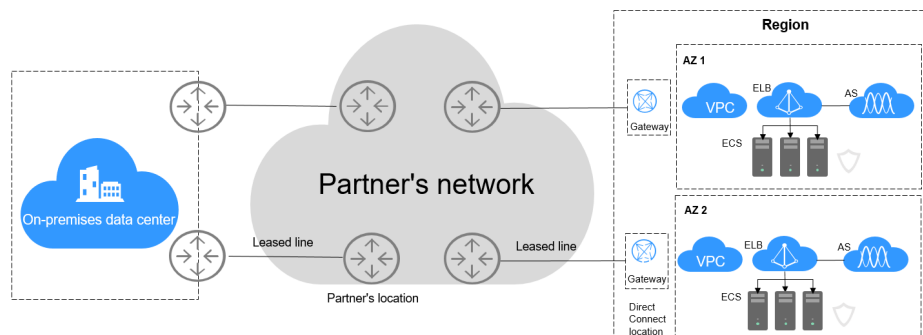
- **Standard connection**
A standard connection provides a dedicated port for your exclusive use. You can create standard connections on the console and create multiple connections terminating at different locations as backups for each other to improve reliability. If, for some reason, there is only one carrier, you can create redundancy by configuring different routes for your connections.

Figure 4-1 Accessing the cloud using standard connections



- **Hosted connection**
If you use a hosted connection to access the cloud, the port you use is shared. After the partner connects to your on-premises data center and Huawei Cloud, the partner provisions a connection for you.

Figure 4-2 Accessing the cloud using hosted connections



Comparison

Item	Standard Connection	Hosted Connection
Port	Exclusive	Shared
Recommended bandwidth	1 Gbit/s to 100 Gbit/s	Less than 1 Gbit/s
Estimated construction period	Two to three months for lines in the same city, and three to four months for lines across cities	About one month
Parties involved	You, leased line carrier, equipment room carrier, and Huawei Cloud	You, leased line carrier, and Huawei Cloud
Process	<ol style="list-style-type: none"> 1. You create a connection on the console to reserve a port. 2. You contact the leased line carrier and supervise the line deployment from your on-premises data center to the equipment room at the location you choose. 3. You contact the carrier operating the equipment room at the location you choose to complete the cabling (if required) and connect the jumper inside the equipment room. 4. Your carrier works with Huawei Cloud to commission access devices. 5. You complete required network configuration on the console, including creating a virtual gateway and virtual interface. 	<ol style="list-style-type: none"> 1. The partner deploys the leased line from your on-premises data center to the location you select. 2. The carrier completes the commissioning of access devices. 3. You complete required network configuration on the console, including creating a virtual gateway and virtual interface.

Item	Standard Connection	Hosted Connection
Pricing	<ul style="list-style-type: none">• Pay for the port (by month or year) to Huawei Cloud.• Pay to the carrier of the equipment room at the location for the cabling inside the equipment room.• Pay to the carrier of your on-premises data center for the cabling inside the equipment room.• Pay to the carrier of the lease line for other work and the bandwidth. For details, see Billing.	<ul style="list-style-type: none">• You do not need to pay for the port to Huawei Cloud.• Pay to the carrier of your on-premises data center for the cabling inside the equipment room.• Pay to the carrier of the lease line for other work and the bandwidth.

Network Requirements

- Your on-premises network must use a single-mode fiber with a 1GE, 10GE, 40GE, or 100GE optical module to connect to the access device in the cloud. In addition, key parameters such as the LC, wavelength, and distance must be aligned with the location. Examples of optical module parameters: 1 GE, LC single-mode, 1,310 nm, and 10 km
- Auto-negotiation for the port must be disabled. Port speed and full-duplex mode must be manually configured.
- 802.1Q VLAN encapsulation must be supported on the entire connection, including intermediate devices.
- Your device must support Border Gateway Protocol (BGP) and BGP MD5 authentication or static routing.
- (Optional) You can configure Bidirectional Forwarding Detection (BFD) on the network.
- The maximum transmission unit (MTU) supported at the physical layer cannot exceed 1,522 bytes (14-byte Ethernet header + 4-byte VLAN tag + 1,500-byte IP datagram + 4-byte frame check sequence). The recommended value is 1500.
- Private IP addresses are recommended both on and off the cloud, and the IP address ranges used for communications cannot overlap.

5 Notes and Constraints

Resource	Default Quota	How to Increase Quota
Number of connections that can be created by an account in each region	10	Submit a service ticket.
Number of virtual gateways that can be created by an account in each region	5	Submit a service ticket.
Number of virtual interfaces that can be created by an account in each region	50	Submit a service ticket.
Number of local subnets for a virtual gateway	50	Increasing the quota is not allowed.
Number of routes for BGP sessions on a virtual interface	100	Submit a service ticket.
Number of remote subnets for a virtual interface	50	Submit a service ticket.

Restrictions on Locations

Before creating a connection, you need to select a location. Note the following restrictions:

- There may be more than one location in each region. In this case, network latency from each location to different AZs in the region should be less than 5 ms.

- If your workloads have demanding requirement for network latency, you can [submit a service ticket](#) to confirm which location is the nearest to the AZ where your cloud servers are running.

Product Use Restrictions

- The CIDR block of the VPC cannot overlap with the CIDR block used by the on-premises network.
The on-premises network cannot use 100.64.0.0/10, 127.0.0.0/8, 169.254.0.0/16, and 224.0.0.0/3 because they are reserved for the VPC service.
- Currently, 1GE and 10GE single-mode optical ports can transmit data up to 10 km. If you need an optical port to transmit data for more than 10 km, or you need a 40GE or 100GE port, you need to purchase the optical modules by yourself.
- If you use a Direct Connect connection to access ELB, you must select **Source IP hash** as the load balancing algorithm and disable sticky sessions for ELB.
- Direct Connect can respond to common ICMP packets (echo packets whose type is 8 and code is 0 and do not carry IP options) for ping detections.
- For each connection, a maximum of 30 ping detections can be performed on the local gateway IP address over the port per second.
- To connect on-premises data centers through enterprise routers, ensure that the on-premises data centers are connected to different devices. For details, [submit a service ticket](#).
- A virtual gateway can be associated with only two different devices.

Construction Notes

- Your construction company must comply with the regulations presented by the equipment room carrier and engineers. In case of any violation, the construction cannot be completed.
- No optical-to-electrical converters can be hosted or installed in the equipment room.
- Network blocking due to state policies or Huawei Cloud management will delay the construction. In the event of such situation, contact your Direct Connect manager.
- The equipment room at a location is operated by a telecom carrier or a third party. If there are fees for connecting your leased line to the equipment room or an in-building cable, pay the fees to the equipment room carrier.
- You need to apply for a Letter of Authorization (LOA) and present the LOA when entering the equipment room for construction.

6 Direct Connect Locations

A Direct Connect location provides access to Huawei Cloud in a region. Before using Direct Connect to access Huawei Cloud, you need to obtain the details about each location.

Direct Connect provides a number of locations for you to choose from. You can request a port when creating a connection.

For more information, [submit a service ticket](#) or contact your Direct Connect manager.

Table 6-1 Direct Connect locations

Geographic Region	City	Region	Location
Europe	Dublin	EU-Dublin	Dublin

7 Billing

You can create a standard connection, which will give you exclusive access to the port. You can also request a hosted connection from a partner and share the port with other users.

Billed Items

- **Standard connection**

The following figure shows the items that you need to pay for a standard connection.

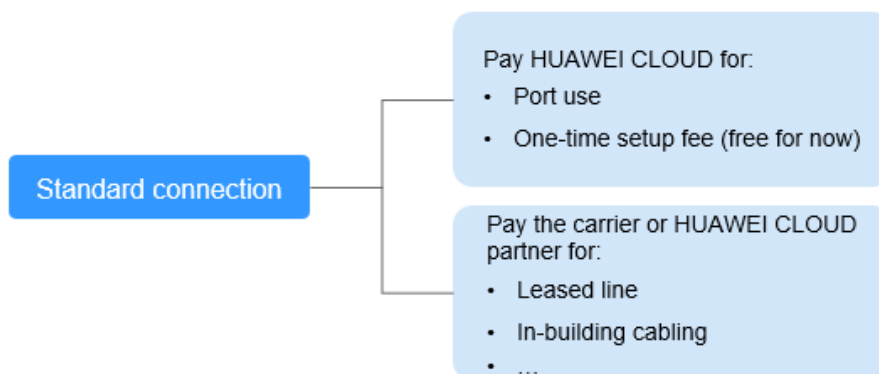


Table 7-1 Standard connection pricing

Payee	Billed Item	Description	Payment Method
Huawei Cloud	Port	The port is billed based on its specifications.	Prepaid (yearly/monthly subscription)
	One-time setup	Currently, the one-time setup is free.	-

Payee	Billed Item	Description	Payment Method
Carrier or Huawei Cloud partner	Leased line	To connect your on-premises data center to the cloud, you need to lease a line from the carrier.	-
	In-building cabling	A fiber may be required for connecting your leased line to the equipment room at the Direct Connect location you select if the data center at the Direct Connect location is a carrier-neutral data center. You pay to the property of the neutral data center.	-

- **Hosted connection**

If you buy a hosted connection from a Huawei Cloud partner, you share the port with other users and do not need to pay for one-time setup and the port to Huawei Cloud.

The following figure shows the billed items of a hosted connection.

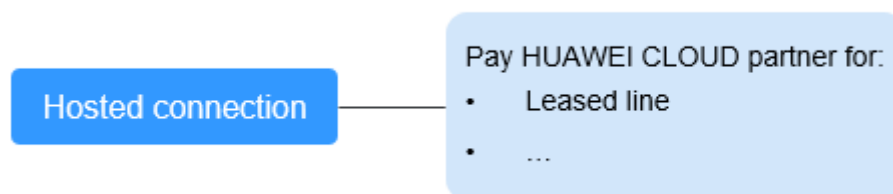


Table 7-2 Hosted connection billing details

Payee	Billed Item	Description	Payment Method
Carrier or Huawei Cloud partner	Leased line	Your partner has established network connectivity with Huawei Cloud. You need to pay for the leased line to the partner.	-

For details, see [Product Pricing Details](#).

Billing Mode

Yearly/Monthly

Changing Billing Mode

Only Yearly/Monthly billing is supported, and it cannot be changed.

Renewal

For details, see [Renewal Management](#).

Expiration and Overdue Payment

For details, see [Service Suspension and Resource Release](#) and [Payment and Repayment](#).

8 Permissions

If you need to assign different permissions to employees in your enterprise to access your Direct Connect resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you securely manage access to your Huawei Cloud resources.

With IAM, you can use your account to create IAM users for your employees, and assign permissions to the users to control their access to specific resource types. For example, some software developers in your enterprise need to use Direct Connect but should not be allowed to delete other Direct Connect resources or perform any other high-risk operations. In this scenario, you can create IAM users for the software developers and grant them only the required permissions.

Skip this part if your account does not require individual IAM users for permissions management.

IAM is a free service. You pay only for the resources in your account. For more information about IAM, see the [What Is IAM?](#)

Direct Connect Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services.

Direct Connect is a project-level service deployed and accessed in specific physical regions. To assign permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing Direct Connect, the users need to switch to a region where they have been authorized to use this service.

You can grant permissions by using roles or policies.

- **Roles:** A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. Only a limited number of service-level roles for authorization are available. When using roles to grant permissions, you need to also assign other roles that the permissions depend

on to take effect. However, roles are not an ideal choice for fine-grained authorization and secure access control.

- **Policies:** A fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, and meets the requirements for secure access control. For example, you can grant Direct Connect users the permissions for only managing a certain type of Direct Connect resources.

Table 8-1 lists all system-defined roles or policies supported by Direct Connect.

Table 8-1 Direct Connect roles or policies

Role/Policy Name	Description	Type	Dependency
Direct Connect Administrator	Has all permissions for Direct Connect resources. To have these permissions, users must also have the Tenant Guest and VPC Administrator permissions.	System-defined role	Tenant Guest and VPC Administrator <ul style="list-style-type: none"> • VPC Administrator: project-level policy, which must be assigned in the same project • Tenant Guest: project-level policy, which must be assigned in the same project
DCaaS Partner	Has permissions of Direct Connect partners. Users who have these permissions can create hosted operations for others. To have these permissions, users must also have the Tenant Guest and VPC Administrator permissions.	System-defined role	Tenant Guest and VPC Administrator <ul style="list-style-type: none"> • VPC Administrator: project-level policy, which must be assigned in the same project • Tenant Guest: project-level policy, which must be assigned in the same project
DCAAS FullAccess	Permissions: all permissions for Direct Connect Scope: project-level service	System-defined policy	None
DCAAS ReadOnlyAccess	Permissions: read-only permissions for Direct Connect Scope: project-level service	System-defined policy	None

Table 8-2 lists common operations supported by each system-defined role or policy for Direct Connect.

Table 8-2 Common operations supported by each system-defined role or policy

Operation	Direct Connect Administrator	DCaaS Partner	DCAAS FullAccess	DCAAS ReadOnlyAccess
Creating a connection	√	√	√	×
Viewing a connection	√	√	√	√
Modifying a connection	√	√	√	×
Deleting a connection	√	√	√	×
Creating a virtual gateway	√	√	√	×
Viewing a virtual gateway	√	√	√	√
Modifying a virtual gateway	√	√	√	×
Deleting a virtual gateway	√	√	√	×
Creating a virtual interface	√	√	√	×
Viewing a virtual interface	√	√	√	√
Modifying a virtual interface	√	√	√	×
Deleting a virtual interface	√	√	√	×
Creating an operations connection	√	√	√	×

Operation	Direct Connect Administrator	DCaaS Partner	DCAAS FullAccess	DCAAS ReadOnlyAccess
Viewing an operations connection	√	√	√	√
Modifying an operations connection	√	√	√	×
Deleting an operations connection	√	√	√	×
Creating a hosted connection	√	√	√	×
Viewing a hosted connection	√	√	√	√
Modifying a hosted connection	√	√	√	×
Deleting a hosted connection	√	√	√	×

Reference

- [What Is IAM?](#)
- [Creating a User and Granting Permissions](#)

9 Direct Connect and Other Services

Figure 9-1 Direct Connect and other services

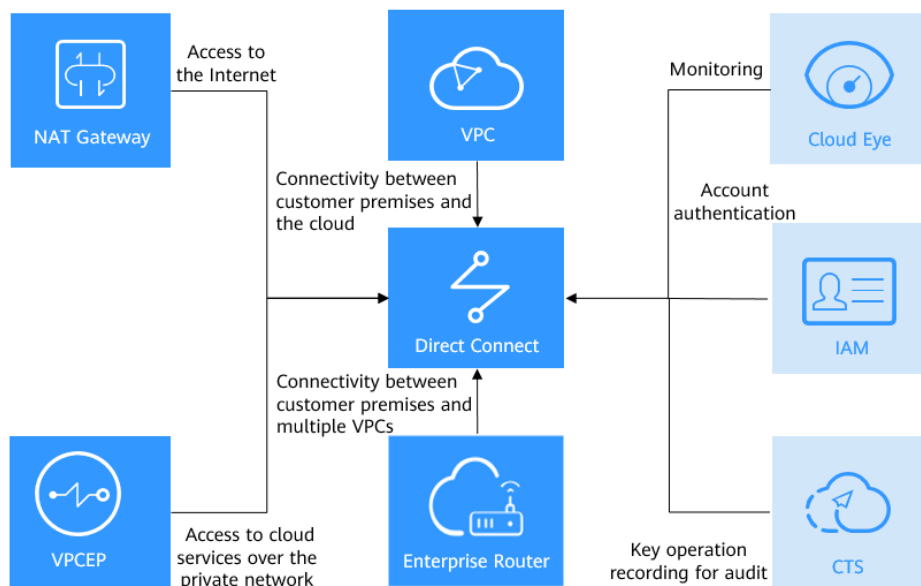


Table 9-1 Related services

Cloud Service	Interaction	Reference
Virtual Private Cloud (VPC)	Your on-premises data center can access the VPCs through Direct Connect.	Creating a VPC
	You can use VPC Peering to connect the VPC your on-premises data center is accessing to other VPCs in the same region so that your on-premises data center can access all these VPCs.	Connecting to Multiple VPCs that Need to Communicate with Each Other

Cloud Service	Interaction	Reference
Enterprise Router	You can connect your on-premises data center to an enterprise router, so that your on-premises data center can access the VPCs attached to the enterprise router.	-
NAT Gateway	On-premises servers can share a NAT gateway to access the Internet or provide services that are accessible from the Internet.	NAT Gateway
VPC Endpoint (VPCEP)	A VPC endpoint can connect your on-premises data center to a cloud service through a VPN or Direct Connect connection over a private network.	Configuring a VPC Endpoint for Accessing OBS Using the OBS Private Address
Cloud Eye	Cloud Eye monitors Direct Connect resources and allows you to view visualized graphs.	Installing Metric Collection Plug-ins
Identity and Access Management (IAM)	You can grant different permissions for users to control access Direct Connect resources.	Identity and Access Management
Cloud Trace Service (CTS)	You can record operations performed on Direct Connect.	Key Operations Recorded by CTS

10 Basic Concepts

10.1 Connection

A connection is dedicated network connection between your on-premises data center and a Direct Connect location over a leased line.

Direct Connect provides ports only. After you request a connection, you need to work with the carrier and Huawei Cloud to establish network connectivity between your on-premises data center and the cloud.

Connections are dedicated channels for on-premises data centers to access the cloud. Connections are more stable, reliable, and secure than Internet-based connections, and provide up to 100 Gbit/s bandwidth.

If you are a regular user, you can request standard connections and hosted connections.

- A standard connection has a dedicated port for your exclusive use and can have multiple virtual interfaces associated.
- A hosted connection is created by a partner and allows you to share the dedicated port with other users. The partner will allocate a VLAN and bandwidth for the hosted connection you request. You can associate only one virtual interface with each hosted connection.

If you are a partner, you can request operations connections and create hosted connections for your users.

- Similar to standard connections, an operations connection has a dedicated port for your exclusive use and can have multiple virtual interfaces associated.
- A hosted connection is created for one of your users based on an operations connection.

If you are a regular user, you need to lease a line from a carrier.

Connections support redundant configuration. If two connections are terminated at different locations in the same region, they work in an active/standby pair to back each other up. If one connection becomes faulty, the other will take over, ensuring stable services.

10.2 Virtual Gateway

A virtual gateway is a logical gateway for accessing a VPC. To access other VPCs, you can use VPC Peering or Cloud Connect to connect the VPC your on-premises data center is accessing to these VPCs.

A virtual gateway can only have one VPC associated. You can link multiple connections to one virtual gateway so that your on-premises data center can access the same VPC.

10.3 Virtual Interface

A virtual interface is what you use to link connections to virtual gateways. A virtual interface can link a connection to one or more virtual gateways so that your on-premises network can access the VPC associated with each virtual gateway.

Virtual interfaces support static routing and BGP routing. You can choose BGP routing if you want to build a hybrid cloud more efficiently and reliably.

10.4 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.

- Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters.

Selecting a Region

If your target users are in Europe, select the **EU-Dublin** region.

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.