

Cloud Connect

Service Overview

Issue 01
Date 2026-03-06



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2026. 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 Cloud Connect?	1
2 Advantages	6
3 Application Scenarios	7
4 Functions	10
5 Region Availability	13
5.1 Supported Regions	13
5.2 Geographic Regions and Huawei Cloud Regions	15
5.3 Region and AZ	15
6 Security	18
6.1 Shared Responsibilities	18
6.2 Identity Authentication and Access Control	20
6.3 Auditing and Logging	20
6.4 Resilience	20
6.5 Monitoring Security Risks	20
6.6 Certificates	21
7 Permissions Management	23
8 Notes and Constraints	34
9 Interaction with Other Services	37

1 What Is Cloud Connect?

Cloud Connect provides both cloud connections and central networks that allow you to connect Virtual Private Clouds (VPCs) in different regions, so that these VPCs can communicate over a private network as if they were within the same network. Cloud Connect can also work with Direct Connect to set up a hybrid cloud network that enables on-premises data centers to access the VPCs across regions. You can choose either a cloud connection or a central network based on service requirements.

Table 1-1 Cloud Connect features

Feature	Application Scenarios	Bandwidth	Advantages	Region Availability
Cloud Connection	<ul style="list-style-type: none"> Connect VPCs in different regions to set up a single private network. Connect on-premises data centers to VPCs in different regions to set up a hybrid cloud network. 	You need to buy and bind a bandwidth package to the cloud connection and assign inter-region bandwidths to enable communication between network instances in different regions.	<ul style="list-style-type: none"> Simple networking VPC in different regions can be connected in minutes. VPCs in different regions are connected. 	Cloud Connection Region Availability

Feature	Application Scenarios	Bandwidth	Advantages	Region Availability
Central Network	<ul style="list-style-type: none"> Connect VPCs in different regions by attaching them to enterprise routers in the corresponding regions. Connect on-premises data centers to VPCs in different regions by attaching them to enterprise routers in the corresponding regions. 	You need to buy and bind a global connection bandwidth to the central network and assign cross-site connection bandwidths to enable communication between the resources in different regions.	<ul style="list-style-type: none"> Flexible networking Dynamic routing A variety of attachments and network scenarios Enterprise routers in different regions are connected. 	Central Network Region Availability

Cloud Connection

A cloud connection enables communication between VPCs in different regions and between VPCs and on-premises data centers.

- Connecting VPCs in different regions
In **Figure 1-1**, two VPCs (VPC-A01 and VPC-A02) in region A, two VPCs (VPC-B01 and VPC-B02) in region B, and two VPCs (VPC-C01 and VPC-C02) in region C are connected using a cloud connection. In this way, all the VPCs in the three regions can communicate with each other.
- Connecting on-premises data centers to VPCs in different regions
In **Figure 1-1**, the VPCs in each region are connected over a cloud connection so all the VPCs in the three regions can communicate with each other.
The on-premises data center in each region is connected to the two VPCs in that region over a Direct Connect connection, and the virtual gateways for each on-premises data center are connected over the cloud connection. In this way, the two on-premises data centers can communicate with all the VPCs in the three regions.

Table 1-2 explains some concepts related to cloud connections.

Figure 1-1 How a cloud connection works

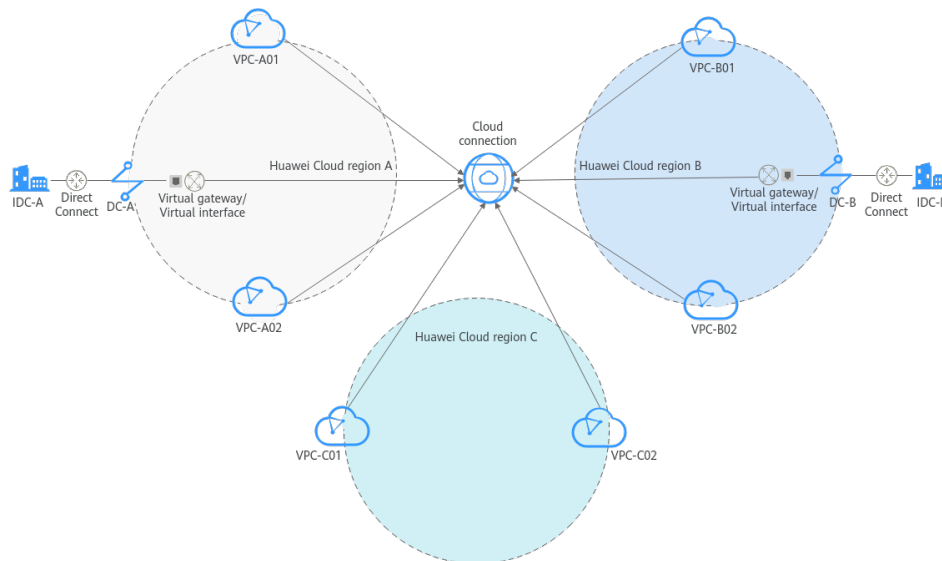


Table 1-2 Cloud connection concepts

Concept	Description
Network instance	<p>A network instance can be a Virtual Private Cloud (VPC) or virtual gateway.</p> <ul style="list-style-type: none"> VPCs in different regions can be connected using a cloud connection. If VPCs are connected by a cloud connection, virtual gateways associated with each VPC can be loaded to this cloud connection to allow the on-premises data center to communicate with these VPCs. <p>In Direct Connect, a virtual gateway associates a virtual interface with a VPC so that the on-premises data center can access this VPC. For more information about Direct Connect, see What Is Direct Connect?</p>
Bandwidth package	<ul style="list-style-type: none"> A bandwidth package is required for inter-region communication regardless of whether: <ul style="list-style-type: none"> The two regions are in the same geographic region. The two regions are in different geographic regions. Bandwidth packages are not required for communication among network instances in the same region. <p>NOTE For details about geographic regions and Huawei Cloud regions, see Geographic Regions and Huawei Cloud Regions.</p>
Inter-region bandwidth	<p>Inter-region bandwidth is used for two regions to communicate with each other. If there is more than one inter-region bandwidth, the sum of all inter-region bandwidths cannot exceed the total bandwidth of the bandwidth package.</p>

Central Network

Relying on the Huawei backbone network, a central network enables communication between enterprise routers, in the same region or across regions, as well as between enterprise routers and on-premises data centers. By applying policies on a central network, you can set up an enterprise-grade network that features flexibility, reliability, and intelligence.

- Connecting VPCs in different regions

In **Figure 1-2**, the two VPCs (VPC-A01 and VPC-A02) are attached to an enterprise router (ER-A) in region A, two VPCs (VPC-B01 and VPC-B02) are attached to an enterprise router (ER-B) in region B, and two VPCs (VPC-C01 and VPC-C02) are attached to an enterprise router (ER-C) in region C.

The three enterprise routers (ER-A, ER-B, and ER-C) are connected over a central network. In this way, the enterprise routers can communicate with each other across regions, and the VPCs in these regions can communicate with each other.

- Connecting on-premises data centers to VPCs in different regions

In **Figure 1-2**, the two VPCs in each region are attached to an enterprise router, and the on-premises data center in each region is connected to the two VPCs in that region over a Direct Connect connection. The global DC gateways for each on-premises data center are attached to the enterprise router in each region, and the enterprise routers in the three regions are connected over the central network.

In this way, the VPCs in all the regions can communicate with each other, and the two on-premises data centers can communicate with all the VPCs in the three regions.

Table 1-3 explains some concepts related to central networks.

Figure 1-2 How a central network works

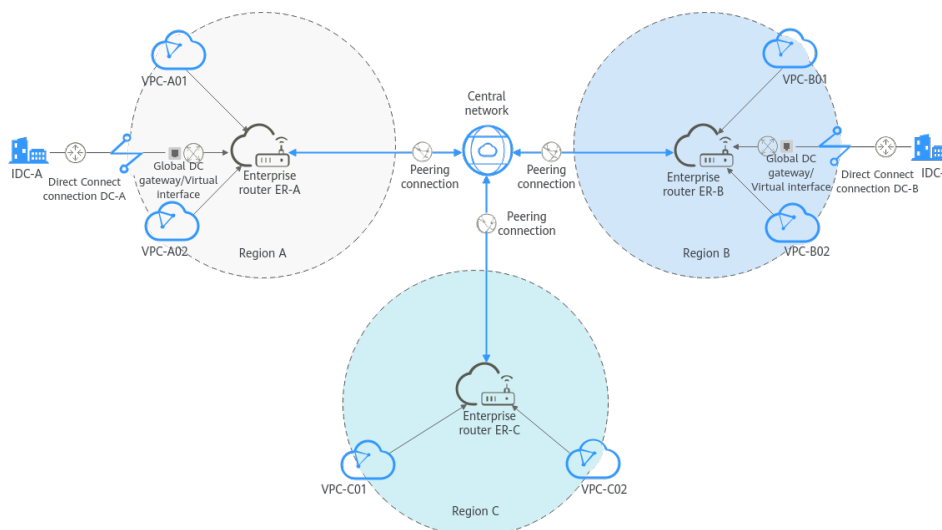


Table 1-3 Central network concepts

Concept	Description
Enterprise router	An enterprise router enables the VPCs in the same region to communicate with each other. By working with global DC gateways provided by Direct Connect, enterprise routers enable the VPCs and on-premises data centers in the same region to communicate with each other. Enterprise routers in different regions can be connected using a central network to allow for cross-region communication between VPCs and between on-premises data centers and VPCs. For more information about enterprise routers, see What Is an Enterprise Router?
Global DC gateway	Global DC gateways can work with enterprise routers to allow on-premises data centers to communicate with the VPCs over a hybrid cloud network. A global DC gateway can be attached to enterprise routers in different regions on a central network. This reduces latency, simplifies network topology, and improves network O&M efficiency.
Global connection bandwidth	A global connection bandwidth can be bound to a central network to allow the resources to communicate with each other over the backbone network, regardless of whether: <ul style="list-style-type: none"> • The resources are in the same geographic region. • The resources are in different geographic regions. For more information, see Geographic-region/Cross-geographic-region Bandwidth Application Scenario (Central Network) .

Accessing Cloud Connect

You can access Cloud Connect through the management console or by calling HTTPS-based APIs.

- Using the management console
The management console is a web-based GUI where you can easily perform various operations. Log in to the [management console](#) and choose **Cloud Connect** from the main menu.
- Using APIs
If you need to integrate Cloud Connect into a third-party system for secondary development, you can use APIs to access Cloud Connect. For details, see the [Cloud Connect API Reference](#).

2 Advantages

Cloud Connect has the following advantages:

- **Full connectivity**
Any two network nodes can be connected, and data packets can be transmitted between them without passing through any other nodes.
- **Ease of use**
In just several simple steps, you can build cross-region VPC connectivity to securely use cloud resources in multiple VPCs.
- **High performance**
Cloud Connect leverages the global network infrastructure of Huawei to provide low-latency and high-quality connectivity. You can flexibly adjust bandwidth to meet your business requirements.
- **Global compliance**
Cloud Connect complies with laws and regulations worldwide, allowing you to focus on business innovation and build business success.

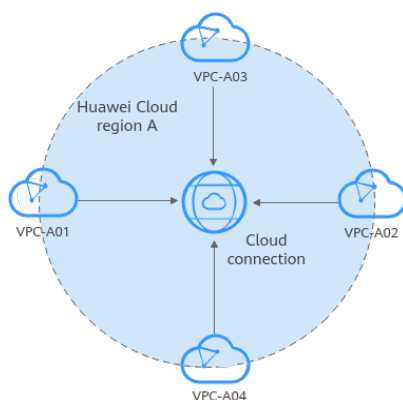
3 Application Scenarios

Cloud Connection Application Scenarios

A cloud connection enables communication between VPCs in different regions and between VPCs and on-premises data centers.

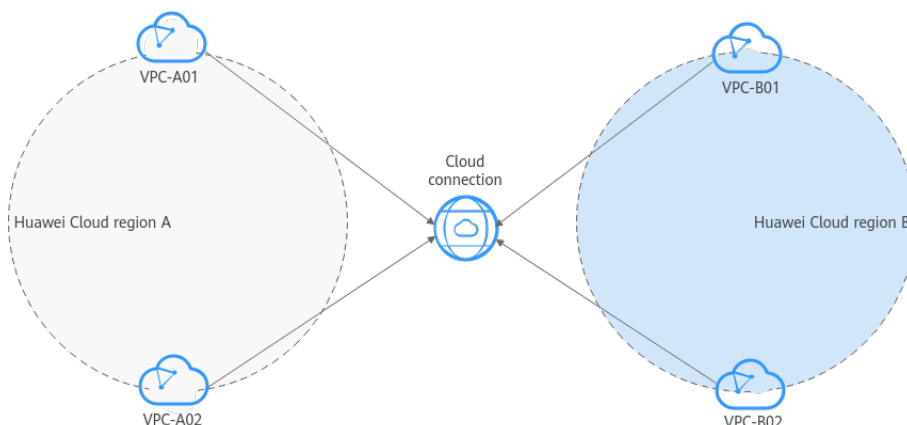
- Connecting VPCs in the same region to set up a single private network
By default, VPCs in the same region can communicate with each other after they are loaded to a cloud connection.

Figure 3-1 Communication between VPCs in the same region



- Connecting VPCs in different regions to set up a private network
With a cloud connection, you can connect VPCs across regions to establish a secure, reliable private network, which improves network topology flexibility.

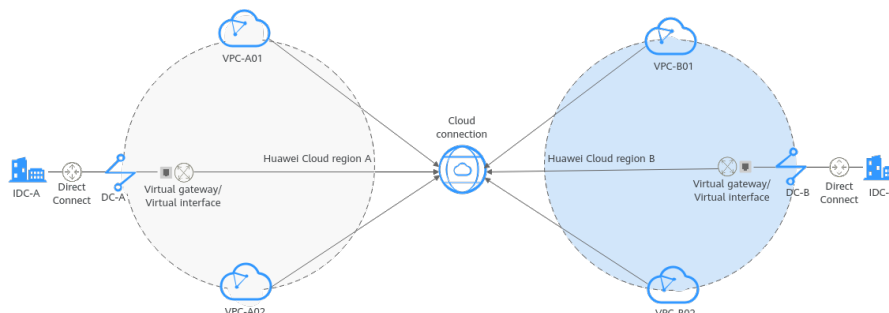
Figure 3-2 Communication between VPCs in different regions



- Connecting on-premises data centers to VPCs in different regions to set up a hybrid cloud network

If you want to establish connectivity between multiple on-premises data centers and VPCs in different regions, you can use Direct Connect to connect each data center to the corresponding VPC and then load all the virtual gateways and VPCs to a cloud connection.

Figure 3-3 Communication between on-premises data centers and VPCs across regions



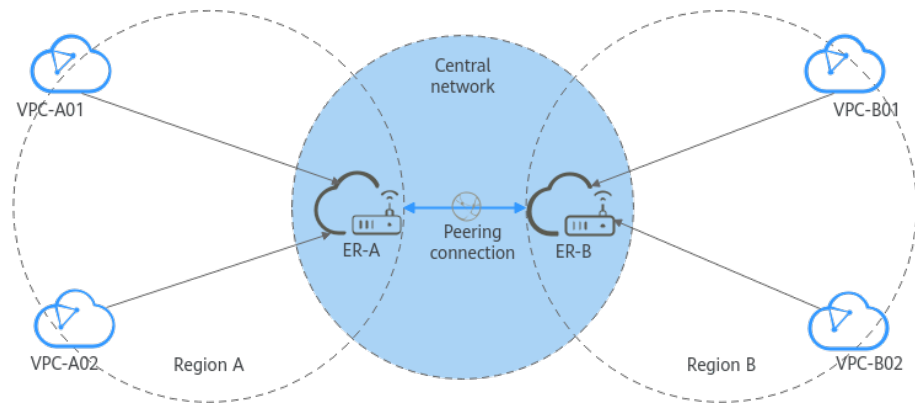
Central Network Application Scenarios

A central network enables enterprise routers in different regions to communicate with each other. It also enables communication between enterprise routers and on-premises data centers, no matter whether they are in the same region or different regions.

- Connecting VPCs in different regions by attaching them to enterprise routers in the corresponding regions

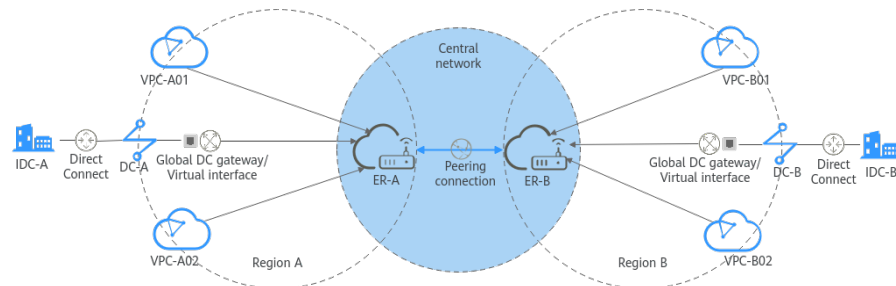
Enterprise routers in different regions are added to a central network as attachments so that resources in these regions can communicate with each other over one network.

Figure 3-4 Cross-region communication between enterprise routers



- Connecting on-premises data centers to VPCs in different regions by attaching them to enterprise routers in the corresponding regions
Enterprise routers and global DC gateways are added to a central network as attachments. In this way, multiple VPCs can communicate with on-premises data centers across regions.

Figure 3-5 Communication between enterprise routers and on-premises data centers



- By flexibly changing the central network policies, you can set up a global network more conveniently.

4 Functions

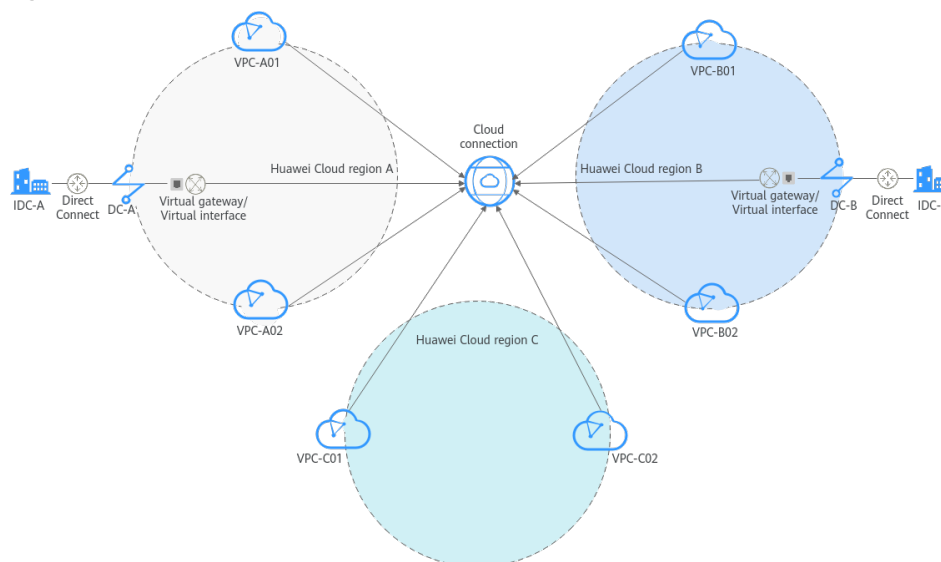
This section describes main functions of Cloud Connect. You can check if a certain function is available in a region on the management console.

Cloud Connection

A cloud connection enables communication between VPCs in different regions and between VPCs and on-premises data centers.

You need to load network instances from these regions to a cloud connection and assign bandwidths for cross-region communication. A network instance can be a VPC you create, a VPC of another user, or a virtual gateway you create for access from your on-premises data center. For details, see [Cloud Connection Overview](#).

Figure 4-1 How a cloud connection works



Network Instance

A network instance can be a VPC you create, a VPC of another user, or a virtual gateway you create for access from your on-premises data center. You need to load network instances to a cloud connection and assign bandwidths for cross-region communication. For details, see [Network Instance Overview](#).

Bandwidth Package

- A bandwidth package is required for inter-region communications regardless of whether:
 - The two regions are within the same geographic region.
 - The two regions are in different geographic regions.
- Bandwidth packages are not required for communications among network instances in the same region.

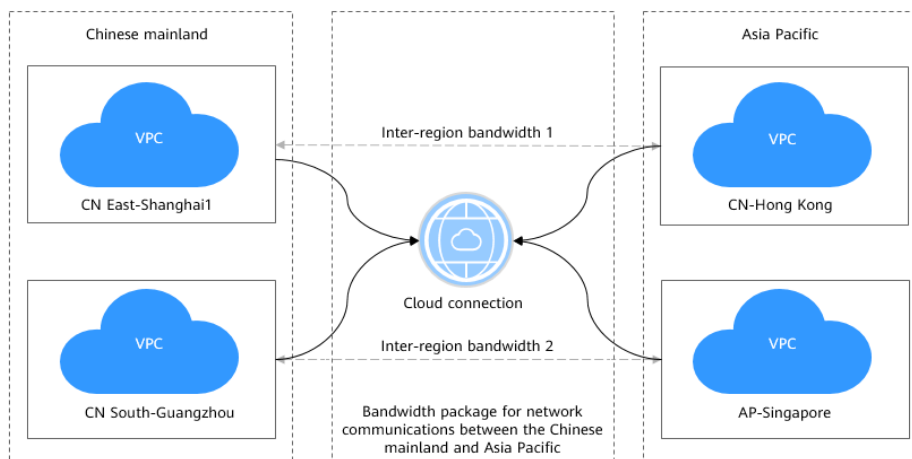
For details, see [Bandwidth Package Overview](#).

Inter-Region Bandwidth

An inter-region bandwidth is used for communications between regions. Inter-region bandwidths are assigned from a bandwidth package for cross-region communications. If there is more than one inter-region bandwidth, the sum of all inter-region bandwidths cannot exceed the total bandwidth of the bandwidth package.

In [Figure 4-2](#), two inter-region bandwidths are assigned from the bandwidth package for communication between the Chinese mainland and Asia Pacific. The sum of the two inter-region bandwidths cannot exceed the maximum bandwidth in the bandwidth package. For details, see [Inter-Region Bandwidth Overview](#).

Figure 4-2 Bandwidth packages and inter-region bandwidths for communications between geographic regions

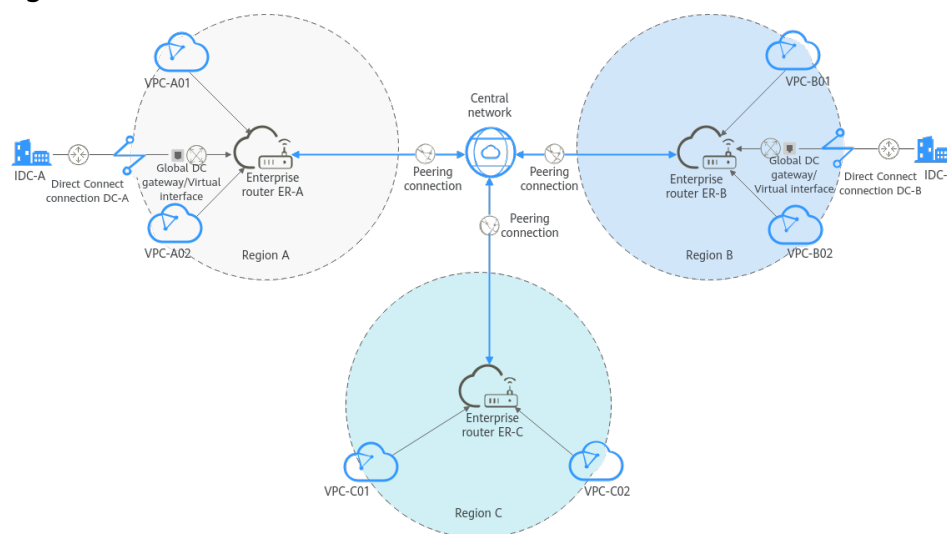


Central Network

Relying on the Huawei backbone network, a central network enables communication between enterprise routers, in the same region or across regions, as well as between enterprise routers and on-premises data centers. By applying policies on a central network, you can set up an enterprise-grade network that features flexibility, reliability, and intelligence.

For details, see [Central Network Overview](#).

Figure 4-3 How a central network works



Global Connection Bandwidth

A global connection bandwidth is used by instances to allow communication over the backbone network.

There are different types of global connection bandwidths that are designed for different application scenarios, including multi-city, HomeZones, geographic-region, and cross-geographic-region bandwidths. Geographic-region and cross-geographic-region bandwidths are often bound to cloud connections for communication on the cloud. For details, see [Global Connection Bandwidth Overview](#).

5 Region Availability

5.1 Supported Regions

This section lists the regions where **cloud connections** and **central networks** are available.

Cloud Connection Region Availability

Table 5-1 lists the regions where cloud connections are available.

Table 5-1 Regions where cloud connections are available

Geographic Region	Huawei Cloud Regions
Chinese mainland	CN North-Beijing4
	CN North-Beijing1
	CN North-Ulanqab1
	CN East-Shanghai1
	CN East-Shanghai2
	CN South-Guangzhou
	CN South-Guangzhou-InvitationOnly
	CN South-Shenzhen
	CN Southwest-Guiyang1
	CN East2 (CN-East-Wuhu)
Asia Pacific	CN-Hong Kong
	AP-Singapore
	AP-Bangkok

Geographic Region	Huawei Cloud Regions
Southern Africa	AF-Johannesburg
Western Latin America	LA-Santiago
Eastern Latin America	LA-Sao Paulo1
Northern Latin America	LA-Mexico City1
	LA-Mexico City2

Central Network Region Availability

Table 5-2 lists the regions where central networks are available.

Table 5-2 Regions where central networks are available

Huawei Cloud Region
CN North-Beijing4
CN North-Ulanqab1
CN East-Shanghai1
CN South-Guangzhou
CN Southwest-Guiyang1
CN East-Qingdao
CN East2 (CN-East-Wuhu)
CN-Hong Kong
AP-Singapore
AP-Bangkok
AP-Jakarta
AP-Manila
AF-Johannesburg
LA-Santiago
LA-Sao Paulo1
LA-Mexico City2
TR-Istanbul
AF-Cairo
ME-Riyadh

5.2 Geographic Regions and Huawei Cloud Regions

Table 5-3 Geographic regions and Huawei Cloud regions

Geographic Region	Huawei Cloud Region
Chinese mainland	CN North-Beijing1
	CN North-Beijing4
	CN East-Shanghai1
	CN East-Shanghai2
	CN South-Guangzhou
	CN East2 When you buy a global connection bandwidth in CN East2, select CN-East-Wuhu for Connect Regions .
Asia Pacific	CN-Hong Kong
	AP-Singapore
	AP-Bangkok
	AP-Jakarta
Southern Africa	AF-Johannesburg
Western Latin America	LA-Santiago
Eastern Latin America	LA-Sao Paulo1
	LA-Buenos Aires1
Northern Latin America	LA-Mexico City1
	LA-Mexico City2
Europe	EU-Dublin

5.3 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.

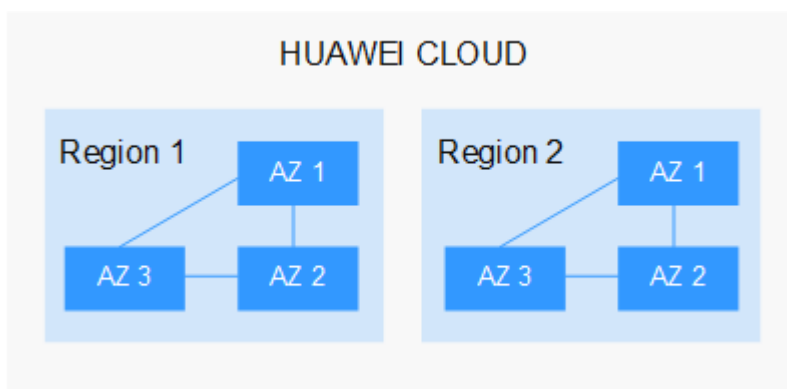
- Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP

(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.

Figure 5-1 shows the relationship between regions and AZs.

Figure 5-1 Regions and AZs



Huawei Cloud provides services in many regions around the world. You can select a region and an AZ based on requirements. For more information, see [Huawei Cloud Global Regions](#).

Selecting a Region

When selecting a region, consider the following factors:

- Location
It is recommended that you select the closest region for lower network latency and quick access.
 - If your target users are in Asia Pacific (excluding the Chinese mainland), select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
 - If your target users are in Africa, select the **AF-Johannesburg** region.
 - If your target users are in Latin America, select the **LA-Santiago** region.

NOTE

The **LA-Santiago** region is located in Chile.

- Resource price
Resource prices may vary in different regions. For details, see [Product Pricing Details](#).

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

6 Security

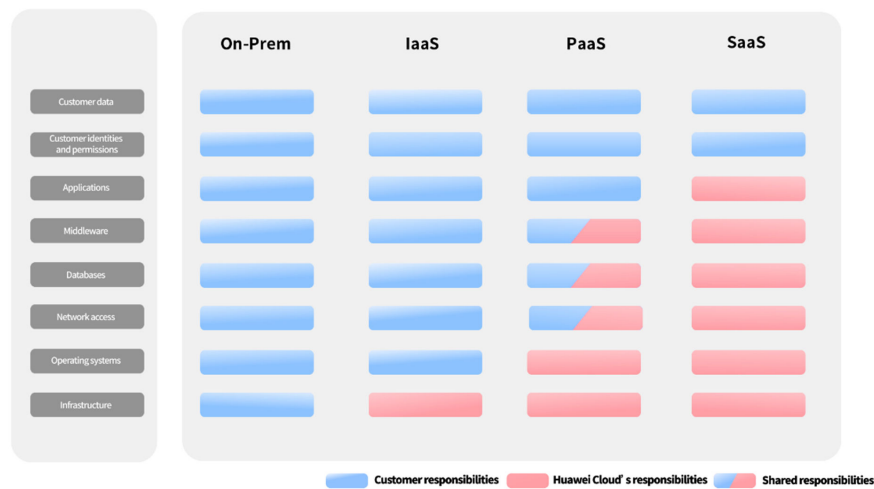
6.1 Shared Responsibilities

Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Unlike traditional on-premises data centers, cloud computing separates operators from users. This approach not only enhances flexibility and control for users but also greatly reduces their operational workload. For this reason, cloud security cannot be fully ensured by one party. Cloud security requires joint efforts of Huawei Cloud and you, as shown in [Figure 6-1](#).

- **Huawei Cloud:** Huawei Cloud is responsible for infrastructure security, including security and compliance, regardless of cloud service categories. The infrastructure consists of physical data centers, which house compute, storage, and network resources, virtualization platforms, and cloud services Huawei Cloud provides for you. In PaaS and SaaS scenarios, Huawei Cloud is responsible for security settings, vulnerability remediation, security controls, and detecting any intrusions into the network where your services or Huawei Cloud components are deployed.
- **Customer:** As our customer, your ownership of and control over your data assets will not be transferred under any cloud service category. Without your explicit authorization, Huawei Cloud will not use or monetize your data, but you are responsible for protecting your data and managing identities and access. This includes ensuring the legal compliance of your data on the cloud, using secure credentials (such as strong passwords and multi-factor authentication), and properly managing those credentials, as well as monitoring and managing content security, looking out for abnormal account behavior, and responding to it, when discovered, in a timely manner.

Figure 6-1 Huawei Cloud shared security responsibility model



Cloud security responsibilities are determined by control, visibility, and availability. When you migrate services to the cloud, assets, such as devices, hardware, software, media, VMs, OSs, and data, are controlled by both you and Huawei Cloud. This means that your responsibilities depend on the cloud services you select. As shown in [Figure 6-1](#), customers can select different cloud service types (such as IaaS, PaaS, and SaaS) based on their service requirements. As control over components varies across different cloud service categories, the responsibilities are shared differently.

- In on-premises scenarios, customers have full control over assets such as hardware, software, and data, so tenants are responsible for the security of all components.
- In IaaS scenarios, customers have control over all components except the underlying infrastructure. So, customers are responsible for securing these components. This includes ensuring the legal compliance of the applications, maintaining development and design security, and managing vulnerability remediation, configuration security, and security controls for related components such as middleware, databases, and operating systems.
- In PaaS scenarios, customers are responsible for the applications they deploy, as well as the security settings and policies of the PaaS middleware, database, and network access under their control.
- In SaaS scenarios, customers have control over their content, accounts, and permissions. They need to protect their content, and properly configure and protect their accounts and permissions in compliance with laws and regulations.

On-premises (On-Prem): Software and IT infrastructure are deployed and managed by customers within their own data centers, rather than be deployed by remote cloud service providers.

Infrastructure as a Service (IaaS): Cloud service providers offer compute, network, storage, and more infrastructure services, including [Elastic Cloud Server \(ECS\)](#), [Virtual Private Network \(VPN\)](#), and [Object Storage Service \(OBS\)](#).

Platform as a Service (PaaS): Cloud service providers deliver platforms required for application development and deployment, such as [ModelArts](#) and [GaussDB](#). Customers do not need to maintain the underlying infrastructure.

Software as a Service (SaaS): Cloud service providers offer complete application software, such as [Huawei Cloud Meeting](#). Customers use the software directly without the need to install the application, maintain it, or manage its underlying platform or infrastructure.

6.2 Identity Authentication and Access Control

You can use Identity and Access Management (IAM) to control access to your Cloud Connect resources. IAM permissions define which actions on your cloud resources are allowed or denied. After creating an IAM user, the administrator needs to add it to a user group and grant the permissions required by Cloud Connect to the user group. And then, all users in this group automatically inherit the granted permissions.

For details, see [Permissions](#).

6.3 Auditing and Logging

Cloud Trace Service (CTS) is a log audit service intended for Huawei Cloud security. It allows you to collect, store, and query cloud resource operation records. You can use these records to perform security analysis, audit compliance, track resource changes, and locate faults.

After CTS is enabled, traces can be generated for Cloud Connect operations.

- For details about how to enable and configure CTS, see [Enabling CTS](#).
- For details about key operations of Cloud Connect, see [Key Operations Recorded by CTS](#).
- For details about traces, see [Viewing Traces](#).

6.4 Resilience

Cloud Connect provides secure private network transmission capabilities based on Huawei's global dedicated network infrastructure. Cloud Connect provides multi-AZ, multi-cluster disaster recovery in more than 20 countries and regions around the world.

Even if some nodes or connections are faulty, the network connectivity will not be interrupted, greatly improving service reliability.

6.5 Monitoring Security Risks

Monitoring is key to ensuring the performance, reliability, and availability of Cloud Connect. Cloud Eye automatically monitors your connections in real time, collects and displays monitoring data in a convenient, visualized manner, and allows you to manage alarms and notifications, helping you watch your cloud connection performance.

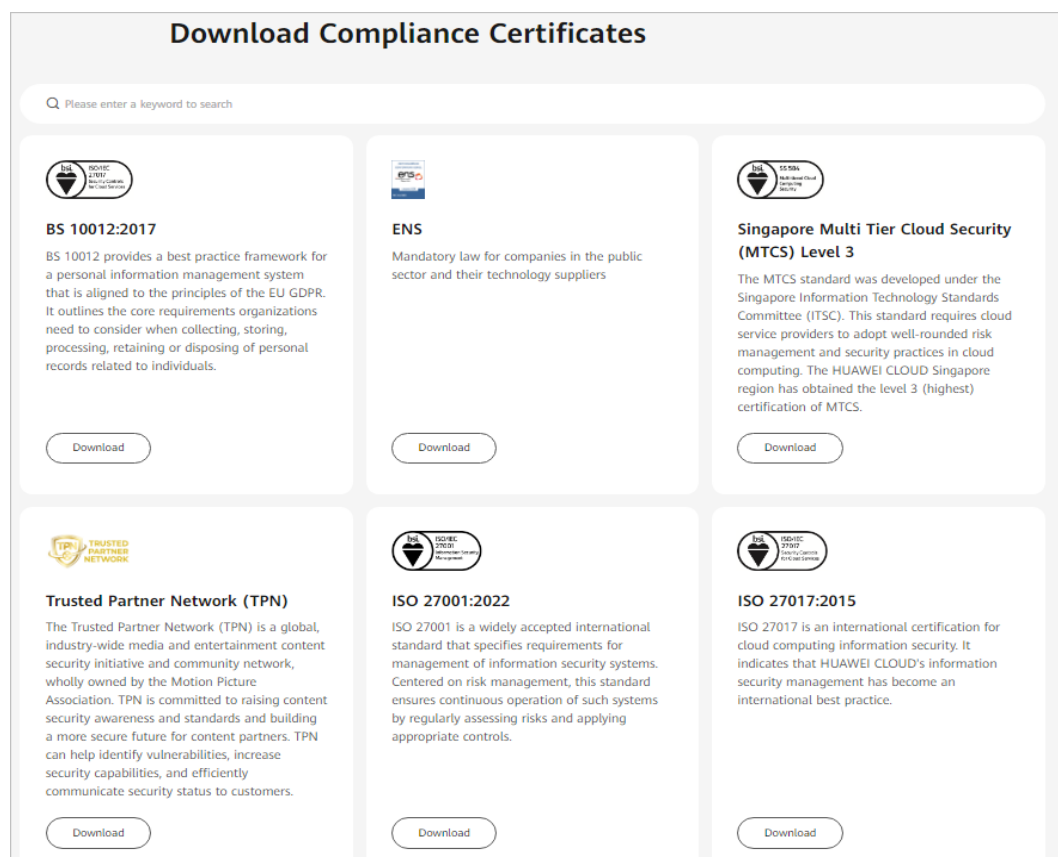
For details about supported metrics and how to create alarm rules, see [Monitoring](#).

6.6 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can [download](#) them from the console.

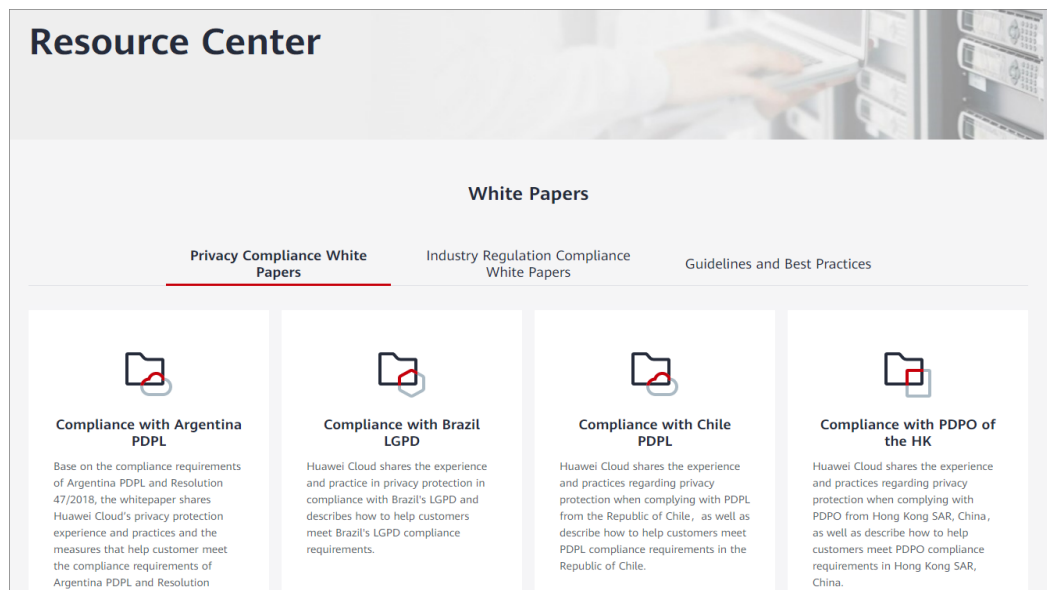
Figure 6-2 Downloading compliance certificates



Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see [Resource Center](#).

Figure 6-3 Resource center



7 Permissions Management

If you need to assign different permissions to personnel in your enterprise to access your Cloud 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 to securely access your Huawei Cloud resources. If your HUAWEI ID does not require IAM for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account.

With IAM, you can control access to specific Huawei Cloud resources. For example, if you want some software developers in your enterprise to use Cloud Connect resources but do not want them to delete the resources or perform any other high-risk operations, you can grant permission to use the resources but not permission to delete them.

IAM supports role/policy-based authorization and identity policy-based authorization.

The following table describes the differences between the two authorization models.

Table 7-1 Differences between role/policy-based authorization and identity policy-based authorization

Name	Authorization Using	Permissions	Authorization Method	Scenario
Role/Policy	User-permission-authorization scope	<ul style="list-style-type: none"> • System-defined roles • System-defined policies • Custom policies 	Assigning roles or policies to principals	To authorize a user, you need to add it to a user group first and then specify the scope of authorization. It is hard to provide fine-grained permissions control using authorization by user groups and a limited number of condition keys. This method is suitable for small- and medium-sized enterprises.
Identity policy	User-policy	<ul style="list-style-type: none"> • System-defined policies • Custom identity policies 	<ul style="list-style-type: none"> • Assigning identity policies to principals • Attaching identity policies to principals 	You can authorize a user by directly attaching an identity policy to it. You can customize policies and attach them to specified users. Identity policies allow you to perform refined access control more efficiently and flexibly. However, this model is more complex and requires higher personnel expertise. It is more suitable for medium- and large-sized enterprises.

Assume that you want to grant IAM users the permission to create ECSs in CN North-Beijing4 and OBS buckets in CN South-Guangzhou. With role/policy-based authorization, the administrator needs to create two custom policies and assign both to the IAM users. With identity policy-based authorization, the administrator only needs to create one custom policy and configure the condition key **g:RequestedRegion** for the policy and attach the policy to the users or grant the users the access permissions to the specified regions. Identity policy-based authorization is more flexible than role/policy-based authorization.

The two authorization models require independent policies and permissions. You are advised to use identity policies for authorization. For details about system-defined permissions, see [Role/Policy-based Permissions Management](#) and [Identity Policy-based Permissions Management](#).

For more information about IAM, see [IAM Service Overview](#).

Role/Policy-based Permissions Management

Cloud Connect supports authorization with roles and policies. New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

Cloud Connect is a global service deployed for all regions. When you set the authorization scope to Global services, users have permission to access Cloud Connect in all regions.

Table 7-2 lists all the system-defined policies for Cloud Connect in role/policy-based authorization. System-defined policies in role/policy-based authorization and identity policy-based authorization are not interoperable.

Table 7-2 System-defined permissions for Cloud Connect

Role/Policy Name	Description	Type	Dependencies
Cross Connect Administrator	Administrator permissions for Cloud Connect. Users with these permissions can perform all operations on Cloud Connect. 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 for the same project • Tenant Guest: project-level policy, which must be assigned for the same project
CC FullAccess	All permissions on Cloud Connect.	System-defined policy	CC Network Depend QueryAccess
CC ReadOnlyAccess	Read-only permissions for Cloud Connect. Users who have these permissions can only view Cloud Connect resources.	System-defined policy	-

Role/Policy Name	Description	Type	Dependencies
CC Network Depend QueryAccess	<p>Read-only permissions required to access dependency resources when using Cloud Connect.</p> <p>Users who have these permissions can view the information of the following resources:</p> <ul style="list-style-type: none"> • VPC • Direct Connect virtual gateway • Enterprise Router 	System-defined policy	-

Table 7-3 lists common operations supported by system-defined permissions.

Table 7-3 Common operations supported by system-defined permissions

Operation	Cross Connect Administrator	CC FullAccess	CC ReadOnlyAccess
Creating a cloud connection	√	√	×
Viewing a cloud connection	√	√	√
Modifying a cloud connection	√	√	×
Deleting a cloud connection	√	√	×
Binding a bandwidth package to a cloud connection	√	√	×
Unbinding a bandwidth package from a cloud connection	√	√	×
Loading a network instance	√	√	×
Viewing a network instance	√	√	√

Operation	Cross Connect Administrator	CC FullAccess	CC ReadOnlyAccess
Updating a network instance	√	√	×
Removing a network instance	√	√	×
Buying a bandwidth package	√	√	×
Viewing a bandwidth package	√	√	√
Modifying a bandwidth package	√	√	×
Unsubscribing from a yearly/monthly bandwidth package	√	√	×
Renewing a yearly/monthly bandwidth package	√	√	×
Assigning an inter-region bandwidth	√	√	×
Viewing an inter-region bandwidth	√	√	√
Modifying an inter-region bandwidth	√	√	×
Deleting an inter-region bandwidth	√	√	×
Viewing monitoring Data of an inter-region bandwidth	√	√	√
Viewing routes	√	√	√
Asking others to authorize the permission to access their VPCs	√	√	×
Viewing authorization	√	√	√
Viewing the other users' VPCs that you are allowed to access	√	√	√

Operation	Cross Connect Administrator	CC FullAccess	CC ReadOnlyAccess
Canceling authorization	√	√	×
Creating a central network	√	√	×
Updating a central network	√	√	×
Deleting a central network	√	√	×
Viewing a central network	√	√	√
Querying central networks	√	√	√
Adding a central network policy	√	√	×
Applying a central network policy	√	√	×
Deleting a central network policy	√	√	×
Querying central network policies	√	√	√
Querying policy changes	√	√	√
Querying central network connections	√	√	√
Updating a central network connection	√	√	×
Adding a global DC gateway to a central network as an attachment	√	√	×
Updating a global DC gateway attachment on a central network	√	√	×

Operation	Cross Connect Administrator	CC FullAccess	CC ReadOnlyAccess
Querying the details of a global DC gateway attachment on a central network	√	√	√
Querying the global DC gateway attachments on a central network	√	√	√
Removing an attachment from a central network	√	√	×
Querying the attachments on a central network	√	√	√
Querying quotas	√	√	√
Querying the capabilities	√	√	√
Creating a global connection bandwidth	√	√	×
Updating a global connection bandwidth	√	√	×
Querying a global connection bandwidth	√	√	√
Deleting a global connection bandwidth	√	√	×

Identity Policy-based Permissions Management

Cloud Connect supports authorization with identity policies. [Table 7-4](#) lists all the system-defined policies for Cloud Connect in identity policy-based authorization. System-defined policies in role/policy-based authorization and identity policy-based authorization are not interoperable.

Table 7-4 Identity policies for Cloud Connect

Policy Name	Description	Policy Type
CCFullAccessPolicy	All permissions on Cloud Connect.	System-defined identity policy
CCReadOnlyPolicy	Read-only permissions for Cloud Connect.	System-defined identity policy

Table 7-5 lists common operations supported by system-defined identity policies of Cloud Connect.

Table 7-5 Common operations supported by each system-defined identity policy of Cloud Connect

Operation	CCFullAccessPolicy	CCReadOnlyPolicy
Creating a cloud connection	√	×
Deleting a cloud connection	√	×
Updating a cloud connection	√	×
Viewing a cloud connection	√	√
Querying cloud connections	√	√
Creating a network instance	√	×
Removing a network instance	√	×
Updating a network instance	√	×
Querying network instance details	√	√
Querying network instances	√	√
Requesting a bandwidth package	√	×
Deleting a bandwidth package	√	×
Updating a bandwidth package	√	×
Querying bandwidth package details	√	√
Querying bandwidth packages	√	√
Binding a bandwidth package	√	×
Unbinding a bandwidth package	√	×

Operation	CCFullAccessPolicy	CCReadOnlyPolicy
Assigning an inter-region bandwidth	√	×
Deleting an inter-region bandwidth	√	×
Updating an inter-region bandwidth	√	×
Querying inter-region bandwidth details	√	√
Querying inter-region bandwidths	√	√
Viewing a cloud connection route	√	√
Querying cloud connection routes	√	√
Querying the quotas	√	√
Querying cloud connection and central network capabilities	√	√
Creating a central network	√	×
Deleting a central network	√	×
Updating a central network	√	×
Querying details of a central network	√	√
Querying central networks	√	√
Adding a central network policy	√	×
Applying a central network policy	√	×
Deleting a central network policy	√	×
Querying central network policies	√	√
Querying the changes between the current policy and the applied policy	√	√
Querying central network connections	√	√

Operation	CCFullAccessPolicy	CCReadOnlyPolicy
Updating a central network connection	√	×
Adding a global DC gateway to a central network as an attachment	√	×
Updating a global DC gateway attachment on a central network	√	×
Querying details of a global DC gateway attachment on a central network	√	√
Querying the global DC gateway attachments on a central network	√	√
Adding an enterprise router route table to a central network as an attachment	√	×
Updating an enterprise router route table added to a central network as an attachment	√	×
Querying details of an enterprise router route table added to a central network as an attachment	√	√
Querying enterprise router route tables added to a central network as an attachment	√	√
Removing an attachment from a central network	√	×
Querying the attachments on a central network	√	×
Creating a global connection bandwidth	√	×
Updating a global connection bandwidth	√	×
Querying a global connection bandwidth	√	√
Deleting a global connection bandwidth	√	×

Roles or Policies that the Cloud Connect Console Depends on

Table 7-6 Roles or policies that the Cloud Connect console depends on

Function	Dependent Cloud Service/Resource	Roles or Policies Required
Assigning cross-site connection bandwidths on a central network	Global connection bandwidth	CCFullAccessPolicy and CC ReadOnlyAccess
Modifying cross-site connection bandwidths on a central network	Global connection bandwidth	CCFullAccessPolicy and CC ReadOnlyAccess
Viewing cross-site connection bandwidths on a central network	Global connection bandwidth	CCFullAccessPolicy and CC ReadOnlyAccess

Helpful Links

- [IAM Service Overview](#)

8 Notes and Constraints

Cloud Connect Constraints

Note the following constraints when you are using Cloud Connect for network communication.

[Cloud Connection Constraints](#)

[Cross-Border Permit Constraints](#)

[Network Instance Constraints](#)

[Bandwidth Package Constraints](#)

[Inter-Region Bandwidth Constraints](#)

[Cross-Account Authorization Constraints](#)

[Route Constraints](#)

[Central Network Constraints](#)

[Global Connection Bandwidth Constraints](#)

Cloud Connection Constraints

- A cloud connection cannot be created between VPCs that have overlapping CIDR blocks, or communication will fail.
- If you load a VPC to a cloud connection created using the same account, you cannot enter loopback addresses, multicast addresses, or broadcast addresses for the custom CIDR block.
- If a NAT gateway has been created for any VPC you have loaded to a cloud connection, a custom CIDR block needs to be added and set to 0.0.0.0/0.
- Multiple bandwidth packages can be bound to a cloud connection only when their billing modes are different.
- A cloud connection can only have one bandwidth package bound if the geographic regions and billing mode of the bandwidth packages are the same.

Central Network Constraints

- To use a central network, the following resources must have been created:
 - Enterprise router: used to build a central network
 - Global DC gateway: attached to an enterprise router for allowing on-premises data centers to access the cloud across regions
- Policy management
 - A central network can only have one policy. If you apply another policy for this central network, the policy that was previously applied will be automatically cancelled.
 - In each policy, only one enterprise router can be added for a region. All added enterprise routers can communicate with each other by default.
 - A policy that is being applied or cancelled cannot be deleted.
- Cross-site connection bandwidth management
 - A cross-site connection bandwidth cannot be changed or deleted when it is being created, updated, deleted, frozen, unfrozen, or is recovering.
 - The total of cross-site connection bandwidths cannot exceed the global connection bandwidth.
 - If a cross-site connection bandwidth is deleted, you will still be billed for the global connection bandwidth.

Cloud Connect Resource Quotas

A quota defines the maximum number of resources of a certain type that can be created in a region or account.

For example, an account can create six central networks by default. If two central networks have been created in the account, four more central networks can be created.

To help you save quotas, there are limits on the maximum number of cloud resources that you can create in each region or account.

You can [log in to the console](#) to view the default quotas for each resource. To increase the resource quota, you can refer to [Applying for a Higher Quota](#).

[Table 8-1](#) and [Table 8-2](#) describe the default quotas of cloud connections and central networks.

Cloud Connection Quotas

Table 8-1 Cloud connection quotas

Item	Default Quota	Adjustable
Cloud connections allowed in each account	6	Yes Submit a service ticket.
Regions per cloud connection	6	Yes Submit a service ticket.

Item	Default Quota	Adjustable
Network instances allowed in each region	6	Yes For cross-region communication, the quota can be increased to 10. Submit a service ticket.
Bandwidth packages for each cloud connection	1	No
Routes per cloud connection	50	Yes Submit a service ticket.

Central Network Quotas

Table 8-2 Central network quotas

Item	Default Quota	Adjustable
Central networks in an account	6	Yes Submit a service ticket.
Policies for a central network	500	Yes Submit a service ticket.
Policy document size (KB)	10	No
Enterprise routers on a central network as attachments in a region	1	No
Global DC gateways on a central network as attachments in a region	3	Yes Submit a service ticket.

9 Interaction with Other Services

Interaction Between Cloud Connections and Other Services

Figure 9-1 How cloud connections interact with other cloud services

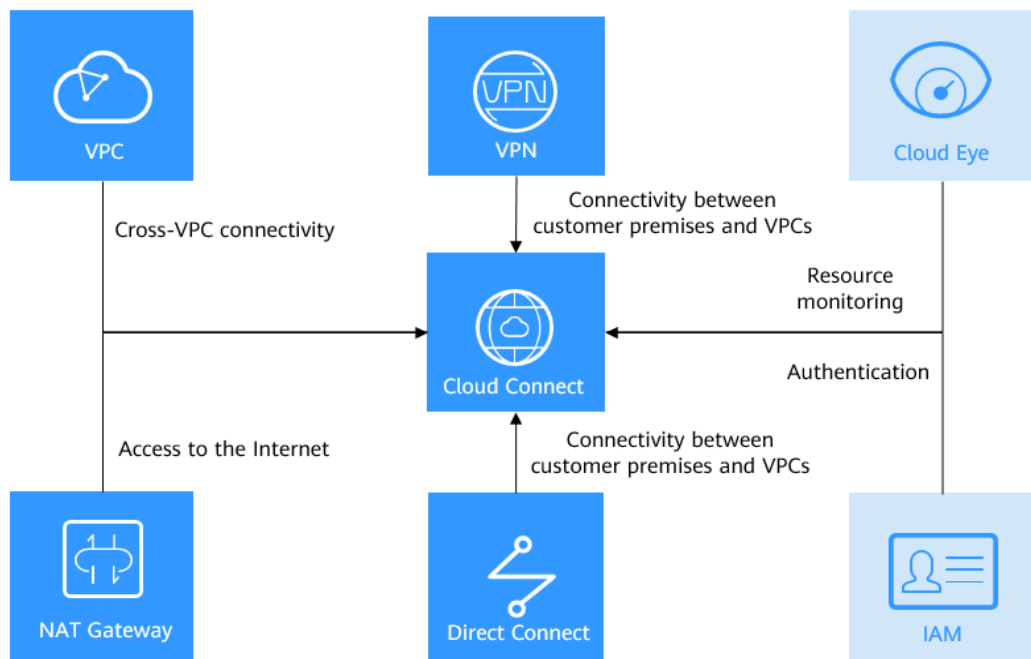


Table 9-1 Interaction between cloud connections and other cloud services

Cloud Service	Interaction	Reference
Virtual Private Cloud (VPC)	VPCs in different regions can be connected over a cloud connection for communication over a private network.	Creating a VPC

Cloud Service	Interaction	Reference
Direct Connect	Cloud connections can work with Direct Connect to connect on-premises data centers to VPCs in different regions.	Connecting On-Premises Data Centers and VPCs in Different Regions
Virtual Private Network (VPN)	Cloud connections can work with VPN to connect on-premises data centers to VPCs in different regions.	-
NAT Gateway	NAT Gateway enables servers in on-premises data centers or VPCs connected by a cloud connection to access the Internet or provide Internet-accessible services.	Working with SNAT to Access the Internet Outside China from a Private Network
Cloud Eye	Cloud Eye monitors cloud connections and allows you to view graphs of metrics.	Viewing Metrics
Identity and Access Management (IAM)	IAM allows you to control access to cloud connection resources.	Identity and Access Management

Interaction Between Central Networks and Other Services

Table 9-2 Interaction between central networks and other cloud services or resources

Cloud Service/ Resource	Interaction	Reference
Enterprise Router	An enterprise router enables the VPCs in the same region to communicate with each other. By working with global DC gateways provided by Direct Connect, enterprise routers enable the VPCs and on-premises data centers in the same region to communicate with each other. Enterprise routers in different regions can be connected using a central network to allow for cross-region communication between VPCs and between on-premises data centers and VPCs.	What's an Enterprise Router?

Cloud Service/ Resource	Interaction	Reference
Global DC gateway	Global DC gateways can work with enterprise routers to allow on-premises data centers to communicate with the VPCs over a hybrid cloud network. A global DC gateway can be attached to enterprise routers in different regions on a central network. This reduces latency, simplifies network topology, and improves network O&M efficiency.	Global DC Gateway Overview
Global connection bandwidth	A global connection bandwidth can be bound to a central network to allow the resources to communicate with each other over the backbone network, regardless of whether: <ul style="list-style-type: none"> • The resources are in the same geographic region. • The resources are in different geographic regions. 	Geographic-Region or Cross-Geographic-Region Bandwidth Application Scenario (Central Network)
Cloud Eye	Cloud Eye monitors central networks and allows you to view graphs of metrics.	Viewing Metrics
IAM	IAM allows you to control access to central networks and related resources.	Identity and Access Management