Cloud Connect

Service Overview

Issue	01
Date	2022-11-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

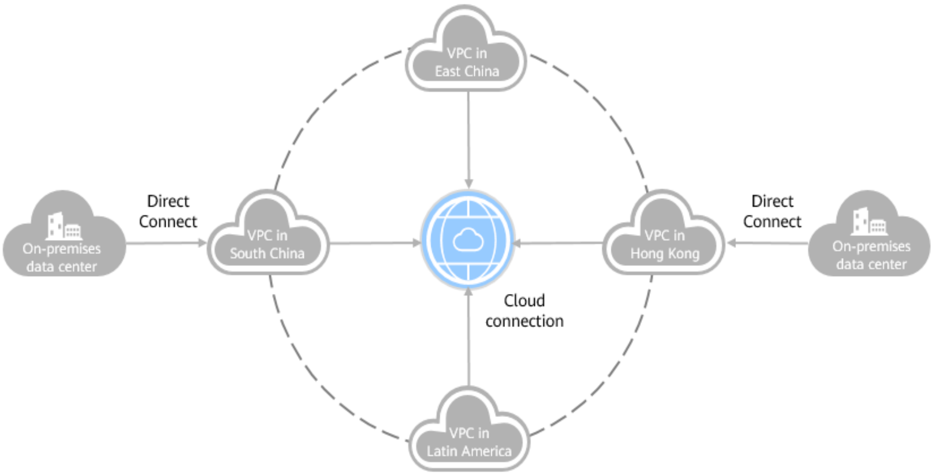
Contents

1 What Is Cloud Connect?

Cloud Connect allows you to connect Virtual Private Clouds (VPCs) in different regions to allow instances in these VPCs to communicate over a private network as if they were within the same network.

You need to load network instances from these regions to a cloud connection and assign bandwidth for cross-region communications. (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.)

Figure 1-1 How Cloud Connect works



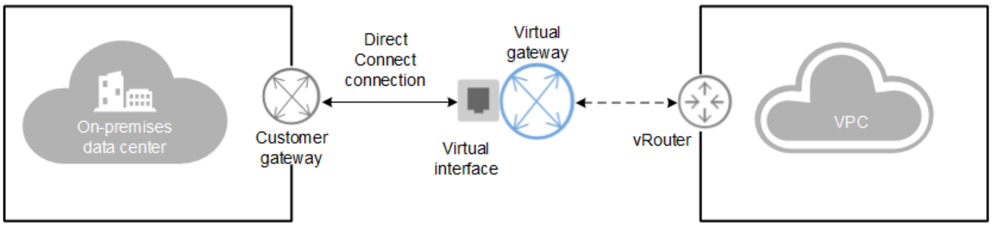
Basic Concepts

Virtual gateway

A virtual gateway functions as a router between your on-premises data center and a VPC on the cloud.

As shown in the figure below, the virtual gateway connects to the VPC on the cloud, and the virtual interface connects the Direct Connect connection to the virtual gateway, so that the on-premises data center can successfully communicate with the VPC.

Figure 1-2 How Direct Connect works



Network instance

A network instance can be a VPC, virtual gateway, or enterprise router.

- VPCs in different regions can be loaded to a cloud connection so that the two VPCs can communicate with each other across regions.
- A virtual gateway can be loaded to a cloud connection to allow the on-premises data center to communicate with one or more VPCs.

Enterprise router

Two or more enterprise routers can be added to a central network for cross-region network communications on the cloud.

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.

Global private bandwidth

A global private bandwidth can be bound to a cloud connection to allow network instances connected using the cloud connection to communicate with each other over the backbone network, regardless of whether:

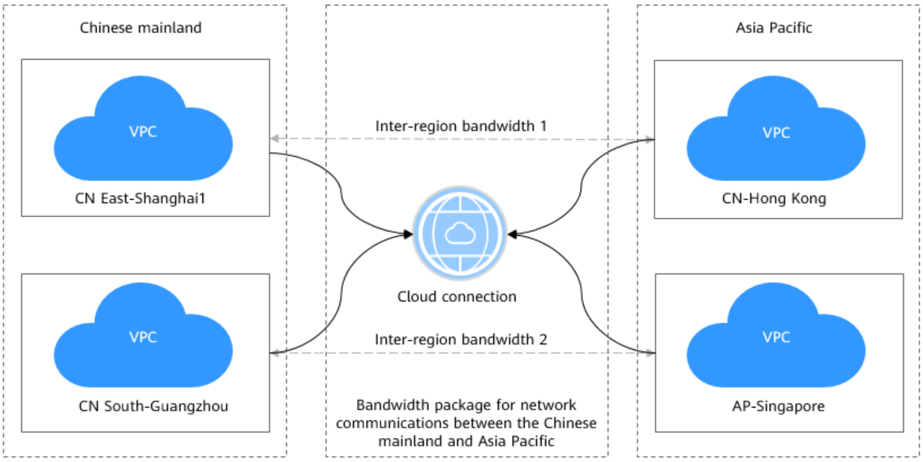
- The network instances are in the same geographic region.
- The network instances are in different geographic regions.

Inter-region bandwidth

Inter-region bandwidth is used for communications between regions. 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 1-3**, two inter-region bandwidths are assigned from the bandwidth package for communications between the Chinese mainland and Asia Pacific. The sum of the two inter-region bandwidths cannot exceed the maximum bandwidth in the bandwidth package.

Figure 1-3 Bandwidth packages and inter-region bandwidths for communications between geographic regions



Accessing Cloud Connect

A web-based user interface is provided for you to access Cloud Connect.

- If you have registered a Huawei Cloud account, log in to the management console and choose **Networking** > **Cloud Connect**.
- If you do not have an account, register an account first by referring to **Preparations**.

2 Advantages

Cloud Connect has the following advantages:

- **Full connectivity**

  Any two network nodes can be connected, and network packages 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.

- **Globally compliant**

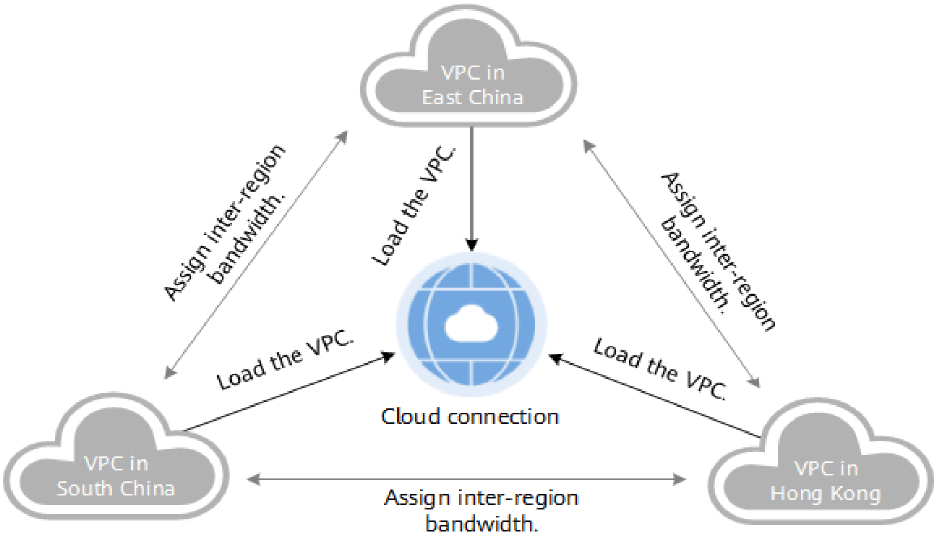
  Cloud Connect complies with laws and regulations worldwide, allowing you to focus on business innovation and build business success.

3 Application Scenarios

Connecting VPCs in Different Regions

Cloud Connect helps you establish secure and reliable private network communications among VPCs in different regions, as shown in **Figure 3-1**. The VPCs can be in your account or another user's account.

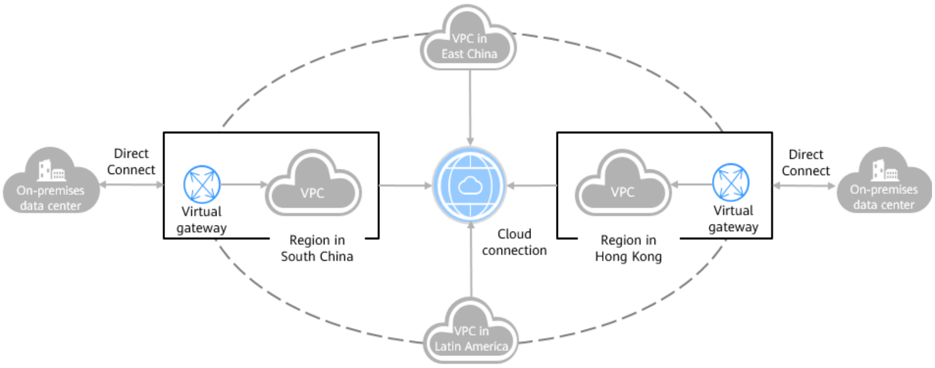
Figure 3-1 Communications among VPCs in different regions



Connecting On-Premises Data Centers to VPCs in Different Regions

If you want to establish connectivity between multiple on-premises data centers and VPCs in different regions, you can use Direct Connect to connect the data centers to a VPC and then load the virtual gateways configured for the data centers and all the VPCs to a cloud connection. The VPCs can be in your account or another user's account.

Figure 3-2 Communications between data centers and VPCs in different regions



4 Constraints

Cloud Connection Constraints

Resource	Quota	How to Increase Quota
Cloud connections allowed in each Huawei Cloud account	6	**Submit a service ticket**.
Regions per a cloud connection	6	**submit a service ticket**.
Network instances allowed in each region	6	**Submit a service ticket**. You can request up to 10 network instances.
Bandwidth packages for each cloud connection	1	The quota cannot be increased.
Routes for a cloud connection	50	**Submit a service ticket**.

⚠ CAUTION

Note the following when you use Cloud Connect:

- A cloud connection cannot be created between VPCs that have overlapping CIDR blocks, or network communications 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.

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 if the cross-site connection is being created, updated, deleted, frozen, recovering, or unfrozen.
  - The total of cross-site connection bandwidths cannot exceed the global private bandwidth.
  - After a cross-site connection bandwidth is deleted, the global private bandwidth will still be billed.

5 Supported Regions

- **Table 5-1** lists the Huawei Cloud regions where Cloud Connect is available.

Table 5-1 Geographic regions and Huawei Cloud regions where Cloud Connect is available

Geographic Region	Huawei Cloud Region
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
Asia Pacific	CN-Hong Kong
	AP-Singapore
	AP-Bangkok
Southern Africa	AF-Johannesburg
Western Latin America	LA-Santiago
Eastern Latin America	LA-Sao Paulo1
Northern Latin America	LA-Mexico City1
	LA-Mexico City2

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

Table 5-2 Huawei Cloud 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-Hong Kong
AP-Singapore
AP-Bangkok
AP-Jakarta
AF-Johannesburg
LA-Santiago
LA-Sao Paulo1
TR-Istanbul

6 Geographic Regions and Huawei Cloud Regions

Table 6-1 Geographic regions and regions

Geographic Region	Region
Chinese mainland	CN North-Beijing1
	CN North-Beijing4
	CN East-Shanghai1
	CN East-Shanghai2
	CN South-Guangzhou
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

7 Billing

Cloud Connect establishes a high-speed, stable, and highly available network among VPCs in different regions. Cloud Connect can work with Direct Connect to enable your on-premises data centers to access VPCs in any region.

To enable communication among network instances in different regions, you need to purchase a bandwidth package. Network instances in the same cloud region can communicate with each other by default and do not require a bandwidth package.

Billing Item

You will be billed only for the bandwidth packages required for cross-region communications.

NOTE

One cloud connection can only have one bandwidth package regardless of if the cloud connection is used for communications within a geographic region or between geographic regions.

Assume that you have created a cloud connection **cc1** and purchased a 50 Mbit/s bandwidth package **bandwidthPackage1** for network communication within the Chinese mainland.

Note that:

- You can bind another bandwidth package to **cc1** only after you unbind **bandwidthPackage1** from **cc1**. If you load network instances in the Asia Pacific to **cc1**, you need to bind one more bandwidth package to enable communications between the Chinese mainland and Asia Pacific.
- If the inter-region bandwidths that you need exceed 50 Mbit/s, increase the bandwidth. For example, if you have assigned 30 Mbit/s for network communications between CN North-Beijing4 and CN East-Shanghai1 and need to assign 40 Mbit/s between CN East-Shanghai1 and CN East-Shanghai2, increase the bandwidth of the package, to no less than 70 Mbit/s.
- A bandwidth package can only be bound to one cloud connection. To change the cloud connection bound to a bandwidth package, unbind the bandwidth package from the cloud connection and bind it to another cloud connection.

For details, see **Product Pricing Details**.

Billing Mode

Yearly/Monthly subscription

Changing Billing Mode

The only billing mode is yearly/monthly, which 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 Security

8.1 Shared Responsibilities

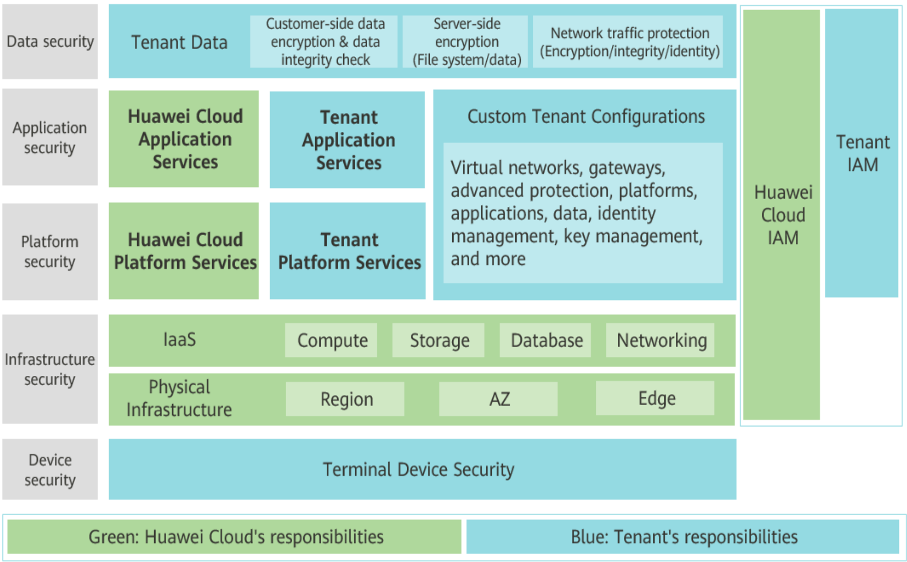
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 8-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 8-1 Huawei Cloud shared security responsibility model


Data security
Tenant Data
Customer-side data encryption & data integrity check
Server-side encryption (File system/data)
Network traffic protection (Encryption/integrity/identity)
Application security
Huawei Cloud Application Services
Tenant Application Services
Custom Tenant Configurations
Virtual networks, gateways, advanced protection, platforms, applications, data, identity management, key management, and more
Platform security
Huawei Cloud Platform Services
Tenant Platform Services
Infrastructure security
IaaS
Compute
Storage
Database
Networking
Physical Infrastructure
Region
AZ
Edge
Device security
Terminal Device Security
Huawei Cloud IAM
Tenant IAM
Green: Huawei Cloud's responsibilities
Blue: Tenant's responsibilities

8.2 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**.

8.3 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**.

8.4 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.

8.5 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.

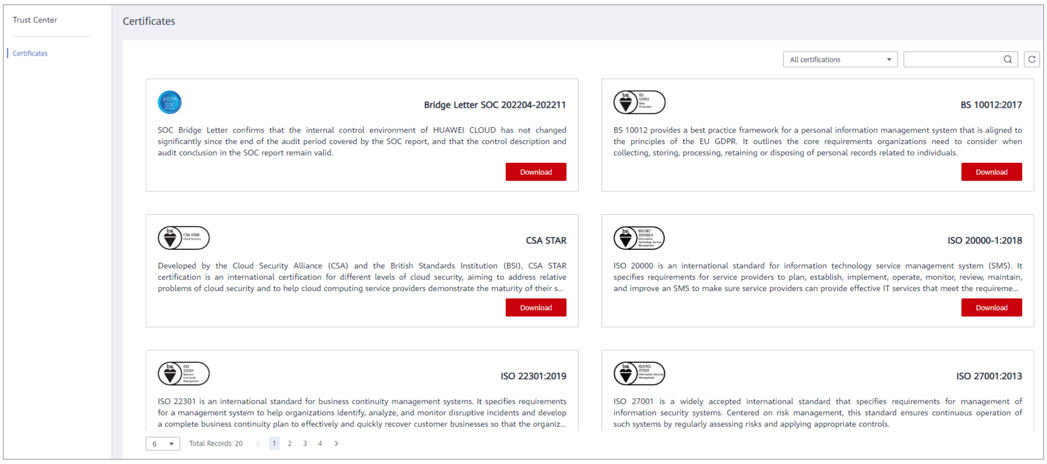
For details about supported metrics and how to create alarm rules, see **Monitoring**.

8.6 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 8-2 Downloading compliance certificates



Bridge Letter SOC 202204-202211

SOC Bridge Letter confirms that the internal control environment of HUAWEI CLOUD has not changed significantly since the end of the audit period covered by the SOC report, and that the control description and audit conclusion in the SOC report remain valid.

BS 10012:2017

BS 10012 provides a best practice framework for a personal information management system that is aligned to the principles of the EU GDPR. It outlines the core requirements organizations need to consider when collecting, storing, processing, retaining or disposing of personal records related to individuals.

CSA STAR

Developed by the Cloud Security Alliance (CSA) and the British Standards Institution (BSI), CSA STAR certification is an international certification for different levels of cloud security, aiming to address relative problems of cloud security and to help cloud computing service providers demonstrate the maturity of their s...

ISO 20000-1:2018

ISO 20000 is an international standard for information technology service management system (SMS). It specifies requirements for service providers to plan, establish, implement, operate, monitor, review, maintain, and improve an SMS to make sure service providers can provide effective IT services that meet the requireme...

ISO 22301:2019

ISO 22301 is an international standard for business continuity management systems. It specifies requirements for a management system to help organizations identify, analyze, and monitor disruptive incidents and develop a complete business continuity plan to effectively and quickly recover customer businesses so that the organiz...

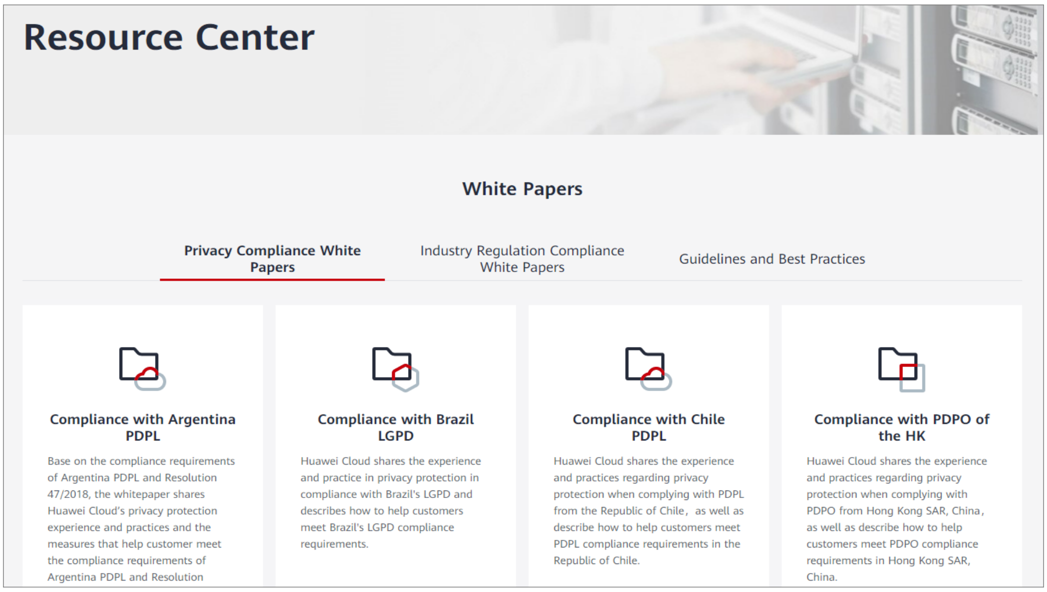
ISO 27001:2013

ISO 27001 is a widely accepted international standard that specifies requirements for management of information security systems. Centered on risk management, this standard ensures continuous operation of such systems by regularly assessing risks and applying appropriate controls.

Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see **Resource Center**.

Figure 8-3 Resource center



Resource Center

White Papers

Privacy Compliance White Papers

Industry Regulation Compliance White Papers

Guidelines and Best Practices

Compliance with Argentina PDPL

Base on the compliance requirements of Argentina PDPL and Resolution 47/2018, the whitepaper shares Huawei Cloud's privacy protection experience and practices and the measures that help customer meet the compliance requirements of Argentina PDPL and Resolution

Compliance with Brazil LGPD

Huawei Cloud shares the experience and practice in privacy protection in compliance with Brazil's LGPD and describes how to help customers meet Brazil's LGPD compliance requirements.

Compliance with Chile PDPL

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPL from the Republic of Chile，as well as describe how to help customers meet PDPL compliance requirements in the Republic of Chile.

Compliance with PDPO of the HK

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPO from Hong Kong SAR, China，as well as describe how to help customers meet PDPO compliance requirements in Hong Kong SAR, China.

9 Permissions

If you need to assign different permissions to employees in your enterprise, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM allows you to control access to your Cloud Connect resources.

With IAM, you can create IAM users for certain employees in your enterprise and assign permissions to control their access to Cloud Connect resources. For example, you can assign permissions to software developers so that they use Cloud Connect but cannot delete Cloud Connect resources or perform any other high-risk operations.

Skip this part if you do not require individual IAM users for refined permissions management.

IAM is a free service. For more information about IAM, see the **IAM Service Overview**.

Cloud Connect Permissions

By default, new IAM users do not have permissions assigned. To assign permissions to these new users, add them to one or more groups and attach permissions policies or roles to these groups.

Cloud Connect is a global service for access from any region. You can assign IAM permissions to users in the global service project. In this way, users do not need to switch regions when they access IAM.

You can grant permissions by using roles or policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions based on user responsibility. This mechanism provides only a limited number of service-level roles. When using roles to grant permissions, you may need to also assign other dependency roles. Roles are not an ideal choice for fine-grained authorization.
- Policies: A type of 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, meeting requirements for secure access control. For example, the administrator can grant Cloud Connect users only the permissions for managing cloud connections.

Table 9-1 lists the system-defined roles or policies supported by Cloud Connect.

Table 9-1 Cloud Connect system-defined roles or policies

System Role/ Policy Name	Description	Type	Dependency
Cross Connect Administrator	Has all permissions for Cloud Connect resources. For permissions of this role to take effect, users must also have the **Tenant Guest** and **VPC Administrator** permissions.	System-defined role	**Tenant Guest** and **VPC Administrator** ● **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
CCReadOnlyAccess	Read-only permissions for Cloud Connect resources. Users who have these permissions can only view Cloud Connect resources.	System-defined policy	None
CC Network Depend QueryAccess	Read-only permissions required to access dependency resources when using Cloud Connect. Users who have these permissions can view VPCs or virtual gateways.	System-defined policy	None

Table 9-2 lists common operations supported by each system-defined role.

NOTE

When you configure system policies **CC FullAccess** and **CC ReadOnlyAccess**, select **Global services** for **Scope**. In this case, the two system policies can take effect for network instances, inter-domain bandwidths, and routes.

Table 9-2 Common operations supported by system-defined permissions

Operation	Cross Connect Administrator	CC FullAccess	CCReadOnlyAccess
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	√	√	√
Modifying a network instance	√	√	×
Removing a network instance	√	√	×
Buying a bandwidth package	√	√	×
Viewing a bandwidth package	√	√	√
Modifying the bandwidth	√	√	×
Unsubscribing from a yearly/monthly bandwidth package	√	√	×
Renewing a yearly/monthly bandwidth package	√	√	×
Assigning inter-region bandwidth	√	√	×

Operation	Cross Connect Administrator	CC FullAccess	CCReadOnlyAccess
Viewing inter-region bandwidth	√	√	√
Modifying inter-region bandwidth	√	√	×
Deleting an inter-region bandwidth	√	√	×
Viewing the monitoring data of an inter-region bandwidth	√	√	√
Viewing route information	√	√	√
Asking others to authorize the permission to access their VPCs	√	√	×
Viewing the VPCs that you authorized for access by other users	√	√	√
Viewing the other users' VPCs that you are allowed to access	√	√	√
Canceling authorization	√	√	×
Creating a central network	×	√	×
Updating a central network	×	√	×
Deleting a central network	×	√	×
Querying details of a central network	×	√	√
Querying central networks	×	√	√
Adding a central network policy	×	√	×

Operation	Cross Connect Administrator	CC FullAccess	CCReadOnlyAccess
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	×	√	×
Querying quotas	√	√	√
Querying the capabilities	√	√	√

Reference

- **What Is IAM?**
- **Creating a User and Assigning Permissions**

10 Interaction with Other Services

Figure 10-1 How Cloud Connect interacts with other services

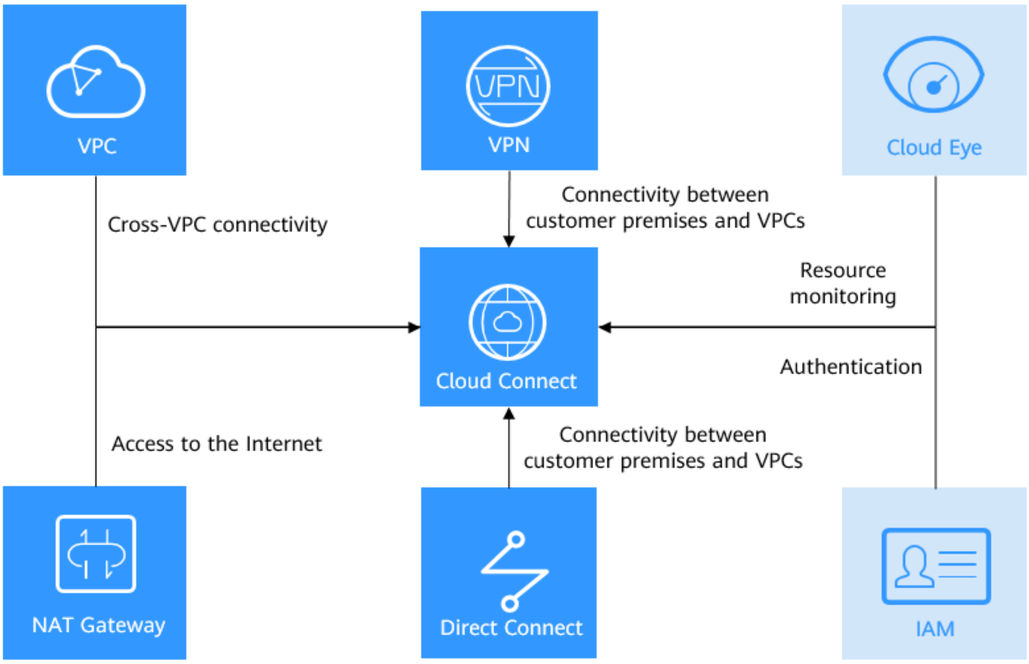


Table 10-1 Interaction between Cloud Connect and other services

Service	Interaction	Reference
Virtual Private Cloud (VPC)	VPCs in different regions can be connected through Cloud Connect for communications over a private network.	**Creating a VPC**
Direct Connect	Cloud Connect can work with Direct Connect to connect on-premises data centers to VPCs in different regions.	**Establishing Communications Between Data Centers and VPCs in Different Regions**

Service	Interaction	Reference
Virtual Private Network (VPN)	Cloud Connect 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 Cloud Connect 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 Connect resources and allows you to view graphs of metrics.	**Viewing Metrics**
Identity and Access Managemen t (IAM)	IAM allows you to control access to Cloud Connect resources.	**Identity and Access Management**

11 Basic Concepts

11.1 Network Instance

A network instance can be a VPC or a virtual gateway.

- VPCs in different regions can be loaded to a cloud connection to enable communications among them.
- If VPCs are connected by a cloud connection, a virtual gateway can be loaded to this cloud connection to allow the on-premises data center to communicate with these VPCs.

11.2 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.

11.3 Global Private Bandwidth

A global private bandwidth can be bound to a cloud connection to allow network instances connected using the cloud connection to communicate with each other over the Huawei Cloud backbone network, regardless of whether:

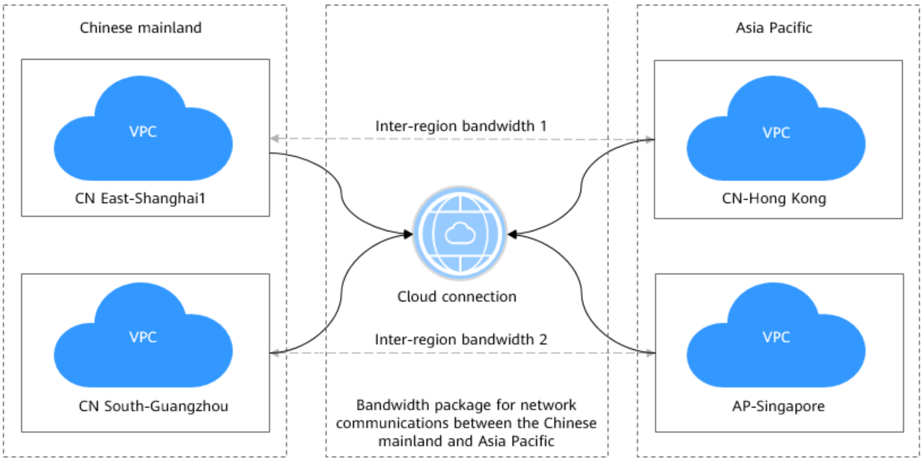
- The network instances are in the same geographic region.
- The network instances are in different geographic regions.

11.4 Inter-Region Bandwidth

Inter-region bandwidth is used for communications between regions. 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 11-1**, two inter-region bandwidths are assigned from the bandwidth package for communications between the Chinese mainland and Asia Pacific. The sum of the two inter-region bandwidths cannot exceed the maximum bandwidth in the bandwidth package.

Figure 11-1 Bandwidth packages and inter-region bandwidths for communications between geographic regions


Chinese mainland
Asia Pacific
VPC
CN East-Shanghai1
Inter-region bandwidth 1
VPC
CN-Hong Kong
Cloud connection
VPC
CN South-Guangzhou
Inter-region bandwidth 2
VPC
AP-Singapore
Bandwidth package for network communications between the Chinese mainland and Asia Pacific