Cloud Connect

Service Overview

Issue 01

Date 2024-08-23

Contents

1 What Is Cloud Connect?

Central Network

Relying on the cloud backbone network, Central Network allows you to easily build a reliable, intelligent enterprise-grade network and manage global network resources on premises and on the cloud. By building a central network, you can enable communications between enterprise routers, as well as between enterprise routers and your on-premises data center, in the same region or different regions.

Enterprise router

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

Global connection bandwidth

A global connection 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.
- Select this type of bandwidth if you need communications across geographic regions.

Accessing Cloud Connect

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

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 Constraints

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, recovering, or unfrozen.
  - 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.

4 Geographic Regions and Huawei Cloud Regions

Table 4-1 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
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 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 5-1 lists the system-defined roles or policies supported by Cloud Connect.

Table 5-1 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
CC ReadOnlyAccess	Read-only permissions for Cloud Connect. Users who have these permissions can only view Cloud Connect resources.	System-defined policy	-
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	-

Table 5-2 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 5-2 Common operations supported by system-defined permissions

Operation	Cross Connect Administrator	CC FullAccess	CC ReadOnlyAccess
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	×	√	×
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	√	√	√

6 Basic Concepts

6.1 Global Connection Bandwidth

A global connection 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.

6.2 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. to support high-availability systems.

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.