VPC Endpoint

Service Overview

Issue	01
Date	2024-04-30

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Contents

1 What Is VPC Endpoint?

VPC Endpoint is a cloud service that provides secure and private channels to connect your VPCs to VPC endpoint services, including cloud services or your private services. It allows you to plan networks flexibly without having to use EIPs.

Architecture

There are two types of resources: VPC endpoint services and VPC endpoints.

- VPC endpoint services are cloud services or private services that you manually configure in VPC Endpoint. You can access these endpoint services using VPC endpoints.

  For more information, see **VPC Endpoint Services**.
- VPC endpoints are secure and private channels for connecting VPCs to VPC endpoint services.
  - VPC endpoints are classified into interface VPC endpoints and gateway VPC endpoints based on the types of VPC endpoint services they access.
    - **Interface VPC endpoints:** They access interface VPC endpoint services and are elastic network interfaces that have private IP addresses.
    - **Gateway VPC endpoints:** They access gateway VPC endpoint services and serve as gateways with routes configured to distribute traffic to the associated gateway VPC endpoint services.
  - There are professional and basic VPC endpoints. Different editions have different features.
    - **Professional** VPC endpoints were newly released and have been in OBT in the CN East2 region. A VPC endpoint supports up to 10 Gbit/s of bandwidth, IPv4 and IPv6 dual stack, and organization-level policy authorization.
    - **Basic** VPC endpoints are the original VPC endpoints.

  For more information, see **VPC Endpoints**.

Figure 1-1 How VPC Endpoint works

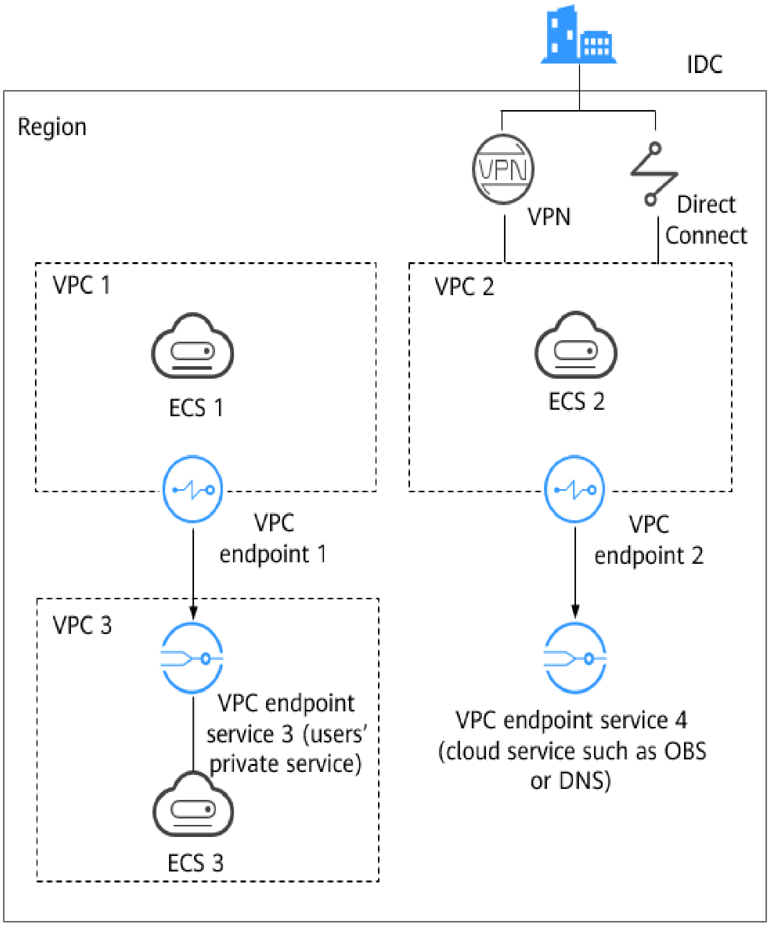

IDC
Region
VPN
Direct Connect
VPC 1
ECS 1
VPC 2
ECS 2
VPC endpoint 1
VPC endpoint 2
VPC 3
VPC endpoint service 3 (users' private service)
ECS 3
VPC endpoint service 4 (cloud service such as OBS or DNS)

Figure 1-1 shows the process of establishing channels for network communications between:

- VPC 1 (ECS 1) and VPC 3 (ECS 3)
- VPC 2 (ECS 2) and cloud services such as OBS and DNS
- IDC and VPC 2 over VPN or Direct Connect to finally access a cloud service such as OBS or DNS

For more information, see **Application Scenarios**.

Accessing VPC Endpoint

You can access VPC Endpoint using any of the following:

- Huawei Cloud management console
  - If you have signed up an account with Huawei Cloud, log in to the management console and choose **Networking** > **VPC Endpoint**.
  - If you do not have an account, create one with Huawei Cloud first by referring to **Preparations**.

  Upon a quick configuration on the management console, you can start using VPC Endpoint.

- APIs

  Use this method if you need to integrate VPC Endpoint into a third-party system for secondary development. For details, see **VPC Endpoint API Reference**.

2 Product Advantages

- **Excellent Performance**: Each gateway supports up to 1 million concurrent connections, meeting requirements in different service scenarios.
- **Ready to Use**: VPC endpoints take effect a few seconds after they are created.
- **Easy to Use**: You can use VPC endpoints to access resources over private networks, without having to use EIPs.
- **High Security**: VPC endpoints enable you to access VPC endpoint services without exposing server information, minimizing security risks.

3 Application Scenarios

VPC Endpoint establishes a secure and private channel between a VPC endpoint (cloud resources in a VPC) and a VPC endpoint service in the same region.

You can use VPC Endpoint in different scenarios.

High-Speed Access to Cloud Services

After you connect an IDC to a VPC using VPN or Direct Connect, you can use a VPC endpoint to connect the VPC to a cloud service or one of your private services, so that the IDC can access the cloud service or private service.

Figure 3-1 Access to cloud services

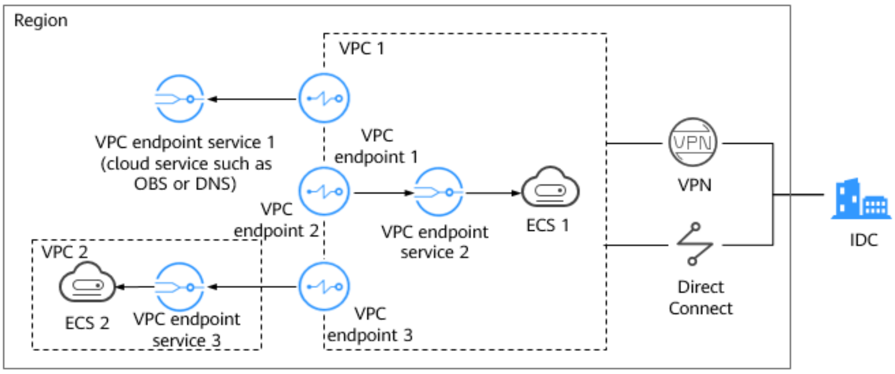


Figure 3-1 shows the process of connecting an IDC to VPC 1 over VPN or Direct Connect, for accessing:

- OBS or DNS using VPC endpoint 1
- ECS 1 in VPC 1 using VPC endpoint 2
- ECS 2 in VPC 2 using VPC endpoint 3

For cloud migration, VPC Endpoint has the following advantages:

- Simple and efficient

  The IDC is directly connected to the VPC endpoint service over a private network, reducing access latency and improving efficiency.

- Low cost

  With VPC Endpoint, your IDC can access cloud resources over a private network, reducing your costs on public resources.

For details, see **Configuring a VPC Endpoint for Accessing the Private IP Address of OBS over Private Networks**.

Cross-VPC Connection

VPC Endpoint enables your resources in two different VPCs within a region to communicate with each other.

NOTE

VPC endpoints and VPC peering connections are different in security, communications methods, route configurations, and more.

For more information, see **What Are the Differences Between VPC Endpoints and VPC Peering Connections?**

Figure 3-2 Cross-VPC connection

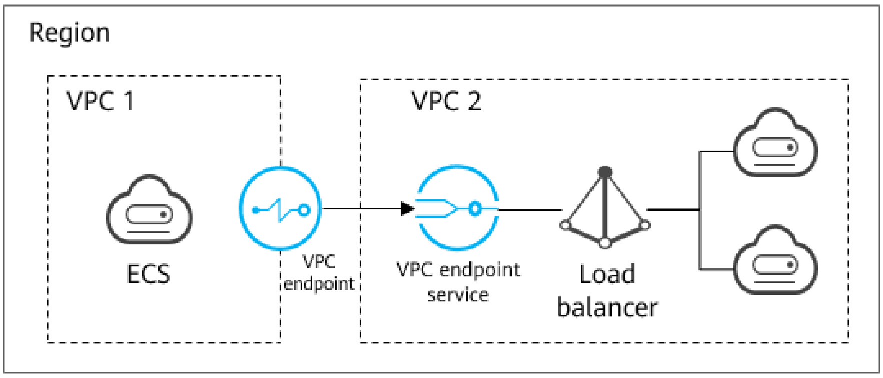


Figure 3-2 shows how an ECS in VPC 1 uses a VPC endpoint to access a load balancer in VPC 2 over a private network.

VPC Endpoint has the following advantages:

- High performance

  Each gateway supports up to one million concurrent connections.
- Simplified operations

  VPC Endpoint resources can be created within seconds and take effect quickly.

For details, see the following sections:

- **Configuring a VPC Endpoint for Communications Across VPCs of the Same Account**
- **Configuring a VPC Endpoint for Communications Across VPCs of Different Accounts**

4 Constraints

Resource Quotas

Table 4-1 describes quotas and constraints on VPC Endpoint resources.

Table 4-1 VPC Endpoint resource quotas and constraints

Resource	Default Quota and Constraints	How to Increase Quota
VPC endpoint services per account in one region	20	Submit a service ticket.
VPC endpoints per account in one region	50	Submit a service ticket.
Traffic types	● **Basic**: indicates the original VPC endpoints, which support IPv4 traffic. ● Professional: IPv4 and IPv6 traffic	N/A

Resource	Default Quota and Constraints	How to Increase Quota
Types of backend resources that can be configured as VPC endpoint services	Load balancer, ECS, and BMS	
Protocols supported by VPC endpoint services	TCP and UDP	

Other Constraints

Basic VPC endpoints:

- When you a VPC endpoint, ensure that the associated VPC endpoint service is deployed in the same region as the VPC endpoint.
- One VPC endpoint can connect to only one VPC endpoint service.
- One VPC endpoint service can have only one backend resource.
- One VPC endpoint supports up to 3,000 concurrent connections.
- One VPC endpoint service can be connected by multiple VPC endpoints.

Professional VPC endpoints:

- Before purchasing a VPC endpoint, ensure that in the same region, there is a VPC endpoint service to be connected.
- One VPC endpoint can connect to only one VPC endpoint service.
- One VPC endpoint service can be connected by multiple VPC endpoints.
- One VPC endpoint service can have only one backend resource.
- One VPC endpoint supports up to 50,000 new connections.
- One VPC endpoint supports up to 1,000,000 concurrent connections.
- One VPC endpoint supports up to 10 Gbit/s of bandwidth.

5 VPC Endpoint and Other Services

Table 5-1 shows the relationship between VPC Endpoint and other cloud services.

Table 5-1 Relationships with other services

Interactive Function	Service	Reference
Creating VPC endpoint services for resources in your VPC	VPC	• Configuring a VPC Endpoint for Communications Across VPCs of the Same Account • Configuring a VPC Endpoint for Communications Across VPCs of Different Accounts
Connecting your on-premises data center to your VPC using a VPN connection and connecting your on-premises data center to a cloud service in another VPC through VPC Endpoint	VPN	Configuring a VPC Endpoint for Accessing the Private IP Address of OBS over Private Networks
Connecting your on-premises data center to your VPC using a Direct Connect connection and connecting your on-premises data center to a cloud service in another VPC through VPC Endpoint	Direct Connect	Configuring a VPC Endpoint for Accessing the Private IP Address of OBS over Private Networks

Interactive Function	Service	Reference
Creating IAM users and controlling their access to VPC Endpoint resources	IAM	**Permissions**
Configured as a gateway VPC endpoint service by default. You can buy a VPC endpoint to access the VPC endpoint service.	OBS	**Buying a VPC Endpoint**
Configured as an interface VPC endpoint service by default. You can buy VPC endpoints to access these endpoint services.	DNS	**Buying a VPC Endpoint**
Configured as an interface VPC endpoint service by default. You can buy VPC endpoints to access these endpoint services.	API Gateway	**Buying a VPC Endpoint**
Configuring a private service as a VPC endpoint service. You can buy a VPC endpoint to access the VPC endpoint service.	ELB	**Creating a VPC Endpoint Service**
Configuring a private service as a VPC endpoint service. You can buy a VPC endpoint to access the VPC endpoint service.	ECS	**Creating a VPC Endpoint Service**
Configuring a private service as a VPC endpoint service. You can buy a VPC endpoint to access the VPC endpoint service.	BMS	**Creating a VPC Endpoint Service**

6 Billing2

Billing Items

VPC Endpoint provides two types of resources: VPC endpoint services and VPC endpoints. VPC endpoint services are free. VPC endpoints are classified into professional and basic VPC endpoints.

- **Professional:** This newly released VPC endpoint type has been in OBT in the CN East2 region and is charged based on the purchased duration and the amount of data processed.

  For professional VPC endpoints, you can set its payer to the VPC endpoint service user or provider. For details, see **Payer Description**.
- **Basic:** VPC endpoints of this original type is charged based on the purchased duration.

The billing mode for VPC endpoints is pay-per-use.

Table 6-1 VPC endpoint billing

Type	Billing Mode	Billing Item	Formula
Professional	Pay-per-use	VPC endpoint price	Pricing per VPC endpoint per hour x Required duration
		Traffic	Pricing per GB of data processed x Data processed
Basic	Pay-per-use	VPC endpoint price	● If the VPC endpoint is used to connect to a DNS or OBS VPC endpoint service, the VPC endpoint is free. ● If the VPC endpoint is not used to connect to a DNS or OBS VPC endpoint service, the VPC endpoint price is calculated as follows: Pricing per VPC endpoint per hour x Required duration

After you purchase a VPC endpoint, you will be charged based on how many hours the VPC endpoint is retained in your account, regardless of whether the VPC endpoint connects to a VPC endpoint service or whether it interacts with the VPC endpoint service.

If the VPC endpoint service is deleted or its owner refuses your VPC endpoint, the VPC endpoint cannot be used but will still be billed. You are advised to delete the VPC endpoint in a timely manner to avoid unnecessary charges.

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

Billing Modes

Pay-per-use

Basic VPC endpoints are billed based on how long (accurate to seconds) the VPC endpoint remains provisioned in your account.

Professional VPC endpoints are billed based on how long (accurate to seconds) the VPC endpoint remains provisioned in your account and the amount of data processed.

Billing Formula

- Basic VPC endpoints: Pricing per VPC endpoint per hour x Required duration
- Professional VPC endpoints: Pricing per VPC endpoint per hour x Required duration + Pricing per GB of data processed x Data processed

For example, if you buy a VPC endpoint and retain it in your account for 5 hours, you will be charged for the 5 hours you keep it.

NOTE

Billing starts after you purchase a VPC endpoint even if you never use it.

Payer Description

VPC Endpoint allows you to authorize other Huawei Cloud accounts to use your own VPC endpoint services. For details, see **Managing Whitelist Records of a VPC Endpoint Service**.

If the professional VPC endpoint you use and the VPC endpoint service it will connect to belong to different Huawei Cloud accounts, you can **submit a service ticket** to set the payer to the VPC endpoint service user or provider.

- **Payment made by the VPC endpoint service user (default):** The VPC endpoint account pays for all fees related to the VPC endpoint.
- **Payment made by the VPC endpoint service provider:** The account to which the VPC endpoint service belongs pays for all fees related to the VPC endpoints connected to it.

Renewal

For details, see **Renewal Management**.

Expiration and Overdue Payment

For details, see **Service Suspension and Resource Release** and **Payment and Repayment**.

7 Security

7.1 Shared Responsibilities

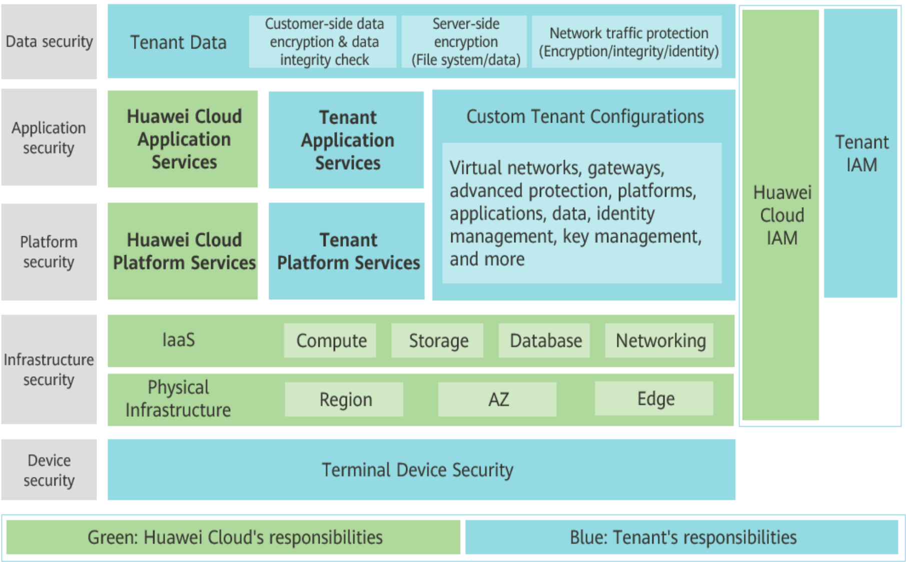
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 7-1 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 7-1 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

7.2 Identity and Access Management

Permissions Management

You can use Identity and Access Management (IAM) to control access to your VPC Endpoint 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 VPC Endpoint to the user group. Then, all users in this group automatically inherit the granted permissions.

For details, see **Permissions**.

Access Control

- To control the access to a VPC endpoint service in one account from a VPC endpoint in another, configure a whitelist for the VPC endpoint service. For details, see **Managing Whitelist Records of a VPC Endpoint Service**.
- To control IP addresses and CIDR blocks that can access a VPC endpoint, configure a whitelist. When or after purchasing a VPC endpoint, you can enable or disable access control for the VPC endpoint, and add or delete a whitelist record. For details, see **Configuring Access Control for a VPC Endpoint**.

7.3 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, it can record VPC Endpoint operations.

- For details about how to enable and configure CTS, see **Enabling CTS**.
- For details about key operations of VPC Endpoint, see **Key Operations Recorded by CTS**.
- For details about traces, see **Viewing Traces**.

7.4 Resilience

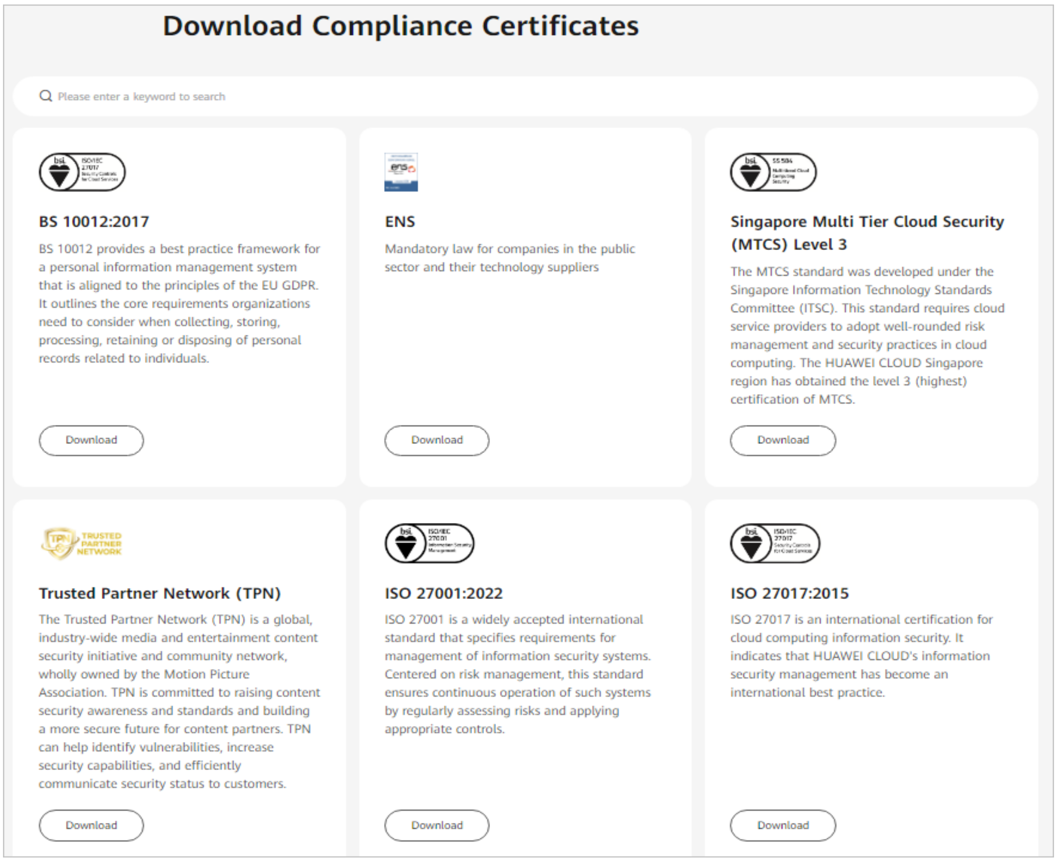
Huawei Cloud VPC Endpoint provides multi-AZ, multi-cluster disaster recovery in more than 20 countries and regions around the world. Even if some nodes, clusters, or regions are faulty, your services will not be interrupted, greatly improving service reliability.

7.5 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 7-2 Downloading compliance certificates



Download Compliance Certificates

Please enter a keyword to search

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.

Download

ENS

Mandatory law for companies in the public sector and their technology suppliers

Download

Singapore Multi Tier Cloud Security (MTCS) Level 3

The MTCS standard was developed under the Singapore Information Technology Standards Committee (ITSC). This standard requires cloud service providers to adopt well-rounded risk management and security practices in cloud computing. The HUAWEI CLOUD Singapore region has obtained the level 3 (highest) certification of MTCS.

Download

Trusted Partner Network (TPN)

The Trusted Partner Network (TPN) is a global, industry-wide media and entertainment content security initiative and community network, wholly owned by the Motion Picture Association. TPN is committed to raising content security awareness and standards and building a more secure future for content partners. TPN can help identify vulnerabilities, increase security capabilities, and efficiently communicate security status to customers.

Download

ISO 27001:2022

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.

Download

ISO 27017:2015

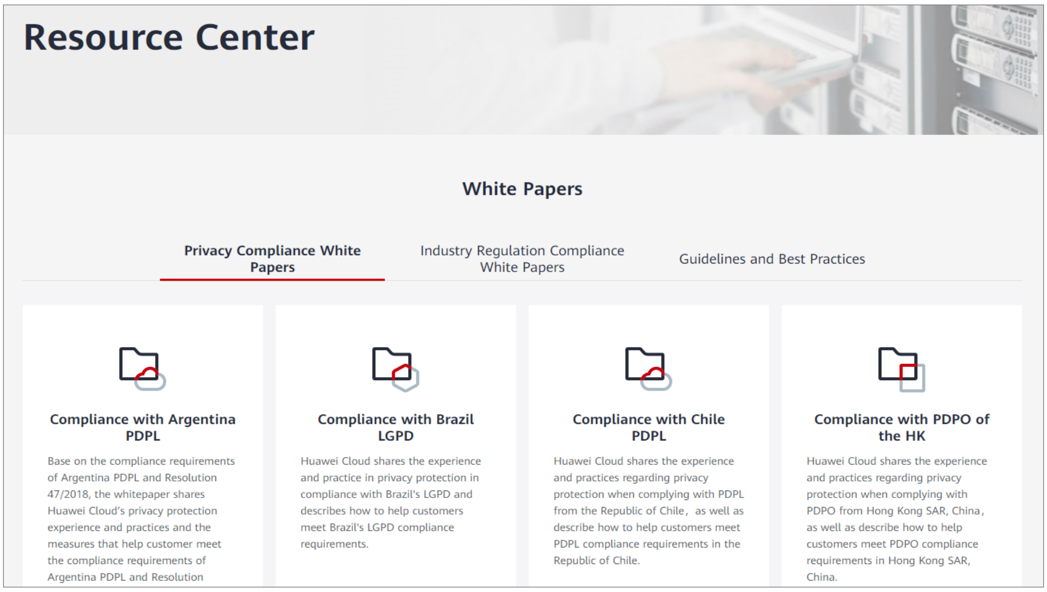
ISO 27017 is an international certification for cloud computing information security. It indicates that HUAWEI CLOUD's information security management has become an international best practice.

Download

Resource Center

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

Figure 7-3 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.

8 Permissions

If you need to assign different permissions to employees in your enterprise to access your VPC Endpoint resources, you can use Identity and Access Management (IAM) to manage fine-grained permissions. IAM provides identity authentication, permissions management, and access control, helping you to securely access your Huawei Cloud resources.

With IAM, you can use your HUAWEI ID to create IAM users and assign permissions to control their access to specific Huawei Cloud resources. For example, if you want website maintenance personnel in your enterprise to use VPC Endpoint resources but do not want them to delete other cloud resources or perform any other high-risk operations, you can create IAM users and grant only permissions to use VPC Endpoint resources.

If your HUAWEI ID does not require individual IAM users for permissions management, you can skip this section.

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

For more information about IAM, see **IAM Service Overview**.

VPC Endpoint Permissions

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.

VPC Endpoint is a project-level service deployed for specific regions. You need to select a project such as **ap-southeast-2** for which the permissions will be granted. If you select **All projects**, the permissions will be granted for all the projects. When accessing VPC Endpoint, the users need to switch to the authorized region.

Table 8-1 lists all system-defined roles for VPC Endpoint.

Table 8-1 System-defined roles for VPC Endpoint

Role	Description	Type	Dependency
VPCEndpoint Administrator	Full permissions for VPC Endpoint	System-defined role	This role depends on **DNS Administrator**, **Server Administrator**, and **VPC Administrator** roles in the same project.

Table 8-2 lists the common operations supported by system-defined permissions for VPC Endpoint.

Table 8-2 Common operations supported by system-defined permissions

Operation	VPCEndpoint Administrator
Creating a VPC endpoint	√
Deleting a VPC endpoint	√
Querying a VPC endpoint	√
Modifying a VPC endpoint	√
Creating a VPC endpoint service	√
Deleting a VPC endpoint service	√
Querying a VPC endpoint service	√
Modifying a VPC endpoint service	√

Helpful Links

- **IAM Service Overview**
- **Creating a User and Granting VPC Endpoint Permissions**

9 Product Concepts

9.1 VPC Endpoint Services

A VPC endpoint service is a cloud service or a private service that can be accessed through a VPC endpoint.

There are two types of VPC endpoint services: gateway and interface.

- Gateway VPC endpoint services are created only for cloud services.
- Interface VPC endpoint services can be created for both cloud services and your private services. Cloud services are configured as VPC endpoint services by the O&M personnel by default. However, you need to create VPC endpoint services for your private services.

Gateway VPC Endpoint Services

Gateway VPC endpoint services are configured from cloud services by the system. You do not have the permissions to configure such VPC endpoint services but can select them when creating a VPC endpoint.

NOTE

Supported cloud services vary in different regions. For details, see the services that can be configured on the management console.

Only in the LA-Mexico City1, LA-Sao Paulo1, and LA-Santiago regions, can OBS be configured as a gateway VPC endpoint service on the VPC Endpoint console.

Table 9-1 Supported gateway VPC endpoint services

VPC Endpoint Service	Category	Type	Example	Description
OBS	Cloud service	Gateway	LA-Mexico City1: com.myhuaweicloud.na-mexico-1.obs	Select the endpoint service ending with **obs** if you want to access OBS using its private address. For details, see **Configuring a VPC Endpoint for Accessing the Private IP Address of OBS over Private Networks**.

Interface VPC Endpoint Services

Interface VPC endpoint services are mainly configured from:

- Cloud services. You do not have the permissions to configure such VPC endpoint services but can select them when creating a VPC endpoint.
- Your private services

NOTE

Supported cloud services vary in different regions. For details, see the services that can be configured on the management console.

Table 9-2 Supported interface VPC endpoint services

VPC Endpoint Service	Category	Type	Example	Description
DNS	Cloud service	Interface	CN-Hong Kong: com.myhuaweicloud.ap-southeast-1.dns	Select the endpoint service ending with **dns** if you want to access DNS over private networks.
API Gateway	Cloud service	Interface	CN-Hong Kong: com.myhuaweicloud.ap-southeast-1.api	Select the endpoint service ending with **api** if you want to access API Gateway using a VPC endpoint.

VPC Endpoint Service	Category	Type	Example	Description
ELB	Users' private service	Interface	None	Select a load balancer as the backend resource if your services receive high traffic and demand high reliability and disaster recovery (DR) performance.
ECS	Users' private service	Interface	None	VPC endpoint services work as servers.
BMS	Users' private service	Interface	None	VPC endpoint services work as servers.

9.2 VPC Endpoints

VPC endpoints are secure and private channels for connecting VPCs to VPC endpoint services.

You can buy a VPC endpoint to connect a resource in your VPC to a VPC endpoint service in another VPC of the same region.

A VPC endpoint comes with a VPC endpoint service. VPC endpoints vary depending on the type of the VPC endpoint services that they can access.

- VPC endpoints for accessing interface VPC endpoint services are elastic network interfaces that have private IP addresses.
- VPC endpoints for accessing gateway VPC endpoint services are gateways, with routes configured to distribute traffic to the associated VPC endpoint services.

A VPC endpoint comes with a VPC endpoint service. VPC endpoints vary depending on the type of the VPC endpoint services that they can access.

- VPC endpoints are classified into interface VPC endpoints and gateway VPC endpoints based on the types of VPC endpoint services they access.
  - **Interface VPC endpoints:** They access interface VPC endpoint services and are elastic network interfaces that have private IP addresses.
  - **Gateway VPC endpoints:** They access gateway VPC endpoint services and serve as gateways with routes configured to distribute traffic to the associated gateway VPC endpoint services.
- There are professional and basic VPC endpoints. Different editions have different features.

- **Professional** VPC endpoints were newly released and have been in OBT in the CN East2 region. A VPC endpoint supports up to 10 Gbit/s of bandwidth, IPv4 and IPv6 dual stack, and organization-level policy authorization.
- **Basic** VPC endpoints are the original VPC endpoints.

NOTE

VPC endpoints for accessing gateway VPC endpoint services can be purchased only in regions LA-Mexico City1, LA-Sao Paulo1, and LA-Santiago.

9.3 User Permissions

The cloud system provides two types of user permissions by default, user management and resource management.

- User management refers to management of users, user groups, and user group permissions.
- Resource management refers to access control over cloud service resources.

VPC Endpoint provides two types of resources: VPC endpoint services and VPC endpoints, both of which are region-level resources. The required permissions must be added for users in the project.

For details about user permissions, see **System Permissions**.

9.4 Region and AZ

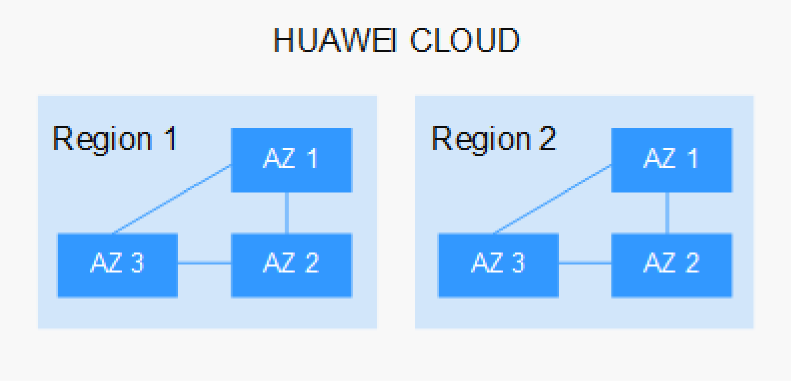
Concept

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. AZs within a region are interconnected using high-speed optical fibers, to support cross-AZ high-availability systems.

Figure 9-1 shows the relationship between regions and AZs.

Figure 9-1 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**.

9.5 Project and Enterprise Project

Project

Projects in IAM are used to group and isolate resources (computing resources, storage resources, and network resources). Resources in your account must be mounted under projects. A project can be a department or a project team. Multiple projects can be created for one account.

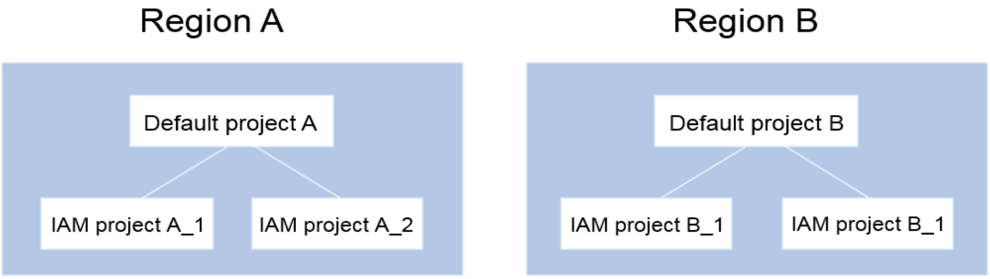
Enterprise Project

Enterprise projects are used to categorize and manage resources. Resources in different regions can belong to one enterprise project. An enterprise can classify resources by department or project group and put relevant resources into one enterprise project for management. Resources can be migrated between enterprise projects.

Differences Between Projects and Enterprise Projects

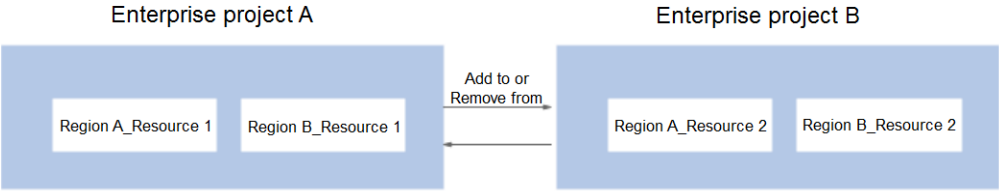
- IAM project

  Projects are used to categorize and physically isolate resources in a region. Resources in an IAM project cannot be transferred. They can only be deleted and then rebuilt.

- Enterprise project

  Enterprise projects are upgraded based on IAM projects and used to categorize and manage resources of different projects of an enterprise. An enterprise project can contain resources of more than one region, and resources can be added to or removed from enterprise projects. If you have enabled enterprise management, you cannot create an IAM project and can only manage existing projects. In the future, IAM projects will be replaced by enterprise projects, which are more flexible.

Both projects and enterprise projects can be managed by one or more user groups. Users who manage enterprise projects belong to user groups. After a policy is granted to a user group, users in the group can obtain the rights defined in the policy in the project or enterprise project.

For details about how to create a project, create an enterprise project, and assign permissions, see **Enterprise Management User Guide**.