Cloud Data Center (CloudDC)

Service Overview

Issue	01
Date	2025-08-01

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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 CloudDC?

Introduction

Cloud Data Center (CloudDC) enables rapid transformation of traditional data centers (DCs) into cloud environments. It allows you to deploy servers in Huawei Cloud equipment rooms, taking advantage of advanced Huawei Cloud capabilities like infrastructure management, cloud-based networking, bare-metal-server management, and deterministic O&M.

Why CloudDC?

- One-stop cloud adoption of compute, networking, and storage: CloudDC offers customizable component combinations to cater to different stages of cloud adoption.
- Full-stack AI infrastructure: CloudDC helps you develop provisioning, cloud-native software stack, and infrastructure optimization capabilities for AI infrastructure. It is tailored to meet the unique needs of AI services.
- Secure and compliant cloud data centers worldwide: CloudDC uses Huawei Cloud's global storage, compute, and networking capabilities to provide stable and secure operating environments for data centers worldwide.
- O&M-free infrastructure management: CloudDC leverages Huawei Cloud's deterministic operations capabilities to make it easier to conduct comprehensive O&M of data center infrastructure, equipment rooms, as well as compute, storage, and networking resources. As you no longer need to worry about the underlying infrastructure, you have more time to focus on your services.

Functions

iRack

CloudDC provides intelligent racks (iRack), highly reliable rack infrastructure that integrates global data center resources. This eliminates the need for investments into site selection, infrastructure construction, and facility construction, accelerating service rollout.

You can access the CloudDC console to query the distribution, quantity, and operating status of racks in real time.

iMetal

iMetal helps manage your servers. You can view basic server information and install operating systems on the iMetal interface. iMetal depends on CloudDCN and the CloudDC O&M platform.

- CloudDCN: You can use CloudDCN to control your network and create VPCs and CloudDCN subnets. CloudDCN provides APIs for iMetal to create network services.
- CloudDC O&M platform: Basic information about iMetal servers is stored and reorganized in the configuration management database (CMDB) of CloudDC so that they are easy to understand on the CloudDC console.

CloudDCN

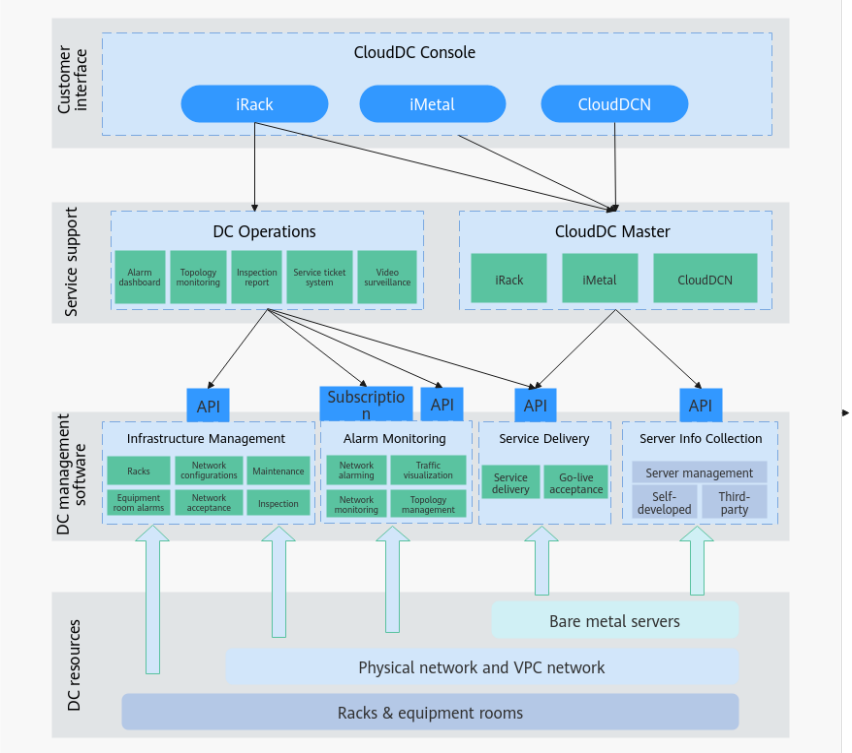
CloudDCN provides network services for CloudDC, including:

- VPC network connectivity via a gateway between the CloudDC zone and Huawei Cloud
- AI parameter-plane network for AI clusters deployed in the CloudDC zone

Architecture

CloudDC uses Huawei Cloud DC capabilities to provide DC management services. The CloudDC architecture consists of four layers, as illustrated in **Figure 1-1**.

Figure 1-1 CloudDC architecture



DC Resources

A Huawei Cloud data center integrates equipment room/rack resources, physical network and VPC network resources, and your bare metal server resources to provide IT infrastructure services.

DC Management Software

- Infrastructure management: This module provides construction and management services for equipment rooms, racks, and network resources.
- Alarm monitoring: This module provides network infrastructure traffic monitoring and topology management, facilitating infrastructure O&M.
- Service delivery: This module conducts engineering implementation and delivery for third-party servers.
- Server information collection: This module manages the operating status of your servers.

Service Support

- DC operations: This supporting part integrates the information presentation of the underlying infrastructure management modules of Huawei Cloud data centers and provides CloudDC O&M capabilities.
- CloudDC Master: This part comprises iRack, iMetal, and CloudDCN. They together provide API calling for the CloudDC console.

CloudDC Console

The CloudDC console integrates iRack, iMetal, and CloudDCN to create a unified operations and management interface. You can monitor the CloudDC status, manage its resources, and perform O&M operations on CloudDC.

Accessing CloudDC

The public cloud provides a web-based service management platform, namely, the management console.

You can access the CloudDC console on the management console.

If you have signed up for the public cloud, log in to the management console and choose **Cloud Data Center** from the service list. If you have not signed up for the public cloud, **sign up for a HUAWEI ID and enable Huawei Cloud services**.

2 Advantages

One-Stop Cloud Adoption of Compute, Networking, and Storage

- You can easily migrate your existing assets to the cloud. The time required for cloud adoption is reduced by a third.
- You can efficiently manage compute, storage, and networking resources through a service-based approach and use them together whenever you need.
- Your servers are deployed in the same equipment room that provides public cloud services, allowing for low-latency access to those public cloud services when you need them.

Full-Stack AI Infrastructure Enablement

- One-stop deployment of AI infrastructure enables efficient collaboration between cloud and edge devices.
- Intelligent racks create an operating environment optimized for AI infrastructure.
- Extensive experience in optimizing AI infrastructure can be leveraged to achieve a linearity of over 90% for a 10,000-card cluster.

Secure and Compliant Cloud Data Centers Worldwide

- CloudDC is accessible in more than 23 AZs, spanning across over 14 countries/regions.
- Huawei Cloud provides extremely reliable Tier 3+ equipment rooms and has systematic data center construction specifications.
- A "One center + Seven layers of defense" security system provides comprehensive and robust security comparable to that on the public cloud.

No O&M Required for Easy Infrastructure Management

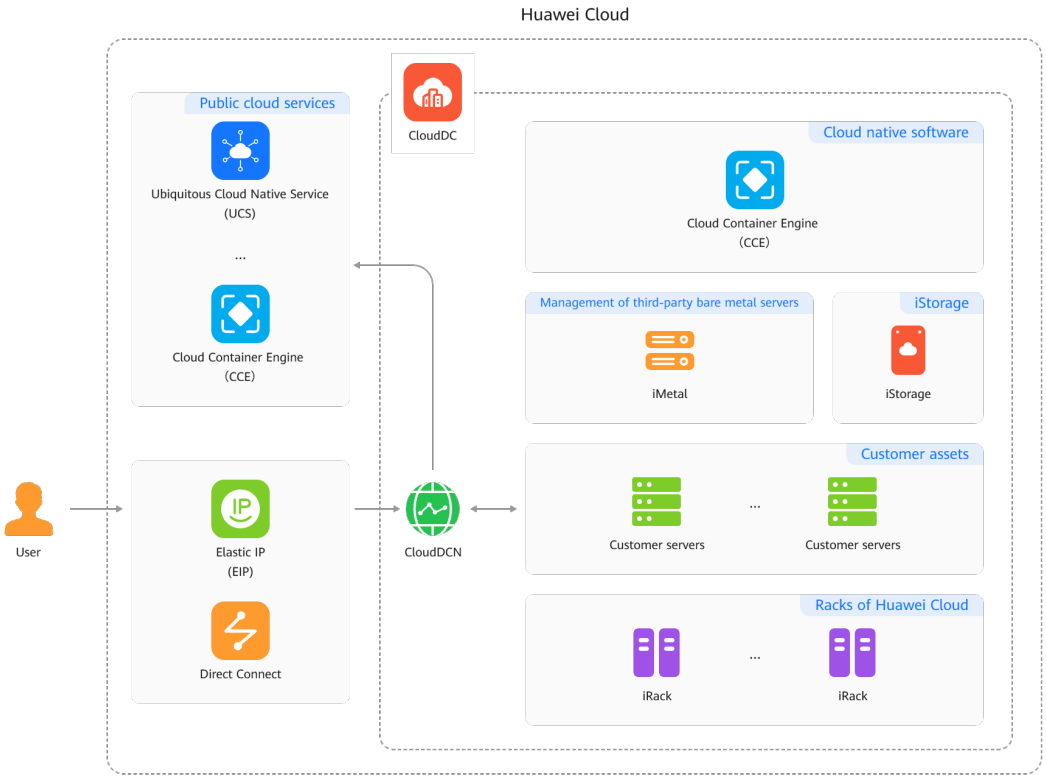
- With over 170 global service centers and 30 years of experience in serving businesses, Huawei is dedicated to providing professional specialized services.
- Infrastructure management is streamlined. 24/7 managed O&M ensures uninterrupted services, so you can focus on your core services.
- You get a clear intuitive view of the status of the data center.

3 Application Scenarios

3.1 DC Cloud Adoption

Scenario

You can manage your assets in data centers with low-latency access to Huawei public cloud services and cloud-based management of data center infrastructure. In addition, Huawei public cloud resources are available for your workloads when there are service peaks in the CloudDC zone.



Benefits

- Low latency: The CloudDC zone is located in an equipment room used for Huawei public cloud services, so you can enjoy the same access latency as on the Huawei public cloud and get seamless access to cloud services.
- High elasticity: The compute resources of the CloudDC zone and the Huawei public cloud are scheduled in a unified manner, and applications running the data center can burst to the public cloud within seconds when the demand for compute capacity spikes.
- Easy management: Huawei Cloud centrally manages the data center facilities, compute and networking resources, as well as container resources.

Key Components

- Intelligent rack (iRack) provides air-cooled intelligent racks.
- Equipment room services (deterministic O&M) include professional services such as assisted O&M, maintenance, security hardening, and engineering delivery.
- Third-party bare metal server management (iMetal) helps you manage your servers and provisions resources in a manner similar to provisioning cloud services such as BMS.
- Network service (CloudDCN) provides the network for the CloudDC zone and connects the zone with Huawei Cloud VPC.

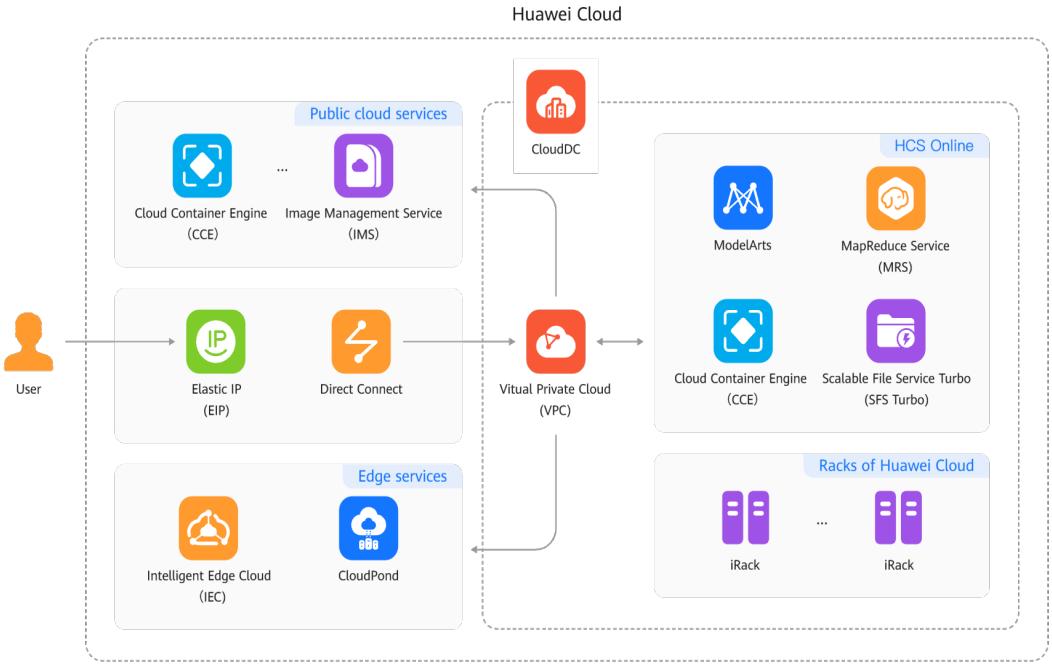
Related Services

- Ubiquitous Cloud Native Service (UCS)
- Cloud Container Engine (CCE)
- Cloud Container Instance (CCI)
- Huawei Cloud EulerOS

3.2 Full-Stack AI

Scenario

You can deploy your AI devices in data centers, where Huawei public cloud's compute, networking, and storage technologies and services are available to smoothly integrate your AI devices with cloud resources. This helps accelerate the deployment of these devices in real business scenarios to enhance efficiency and create value.



Benefits

- High efficiency and security: gPaaS & AI DaaS services are deployed in the CloudDC zone for local data storage and high-speed access.
- Diverse services: More than 110 public cloud services are deployed in the CloudDC zone and can be used on demand.
- Consistent experience: Cloud services running in the CloudDC zone can provide same user experience as those on the public cloud.

Key Components

- iRack provides intelligent racks.
- Equipment room services (deterministic O&M) include consulting, implementation, managed O&M, and optimization of the AI infrastructure.
- Cloud-based AI network (MatrixLink) provides a large-scale, efficient, and highly reliable AI network.
- AI containers (CCE) provide a globally unified environment for AI container operation.

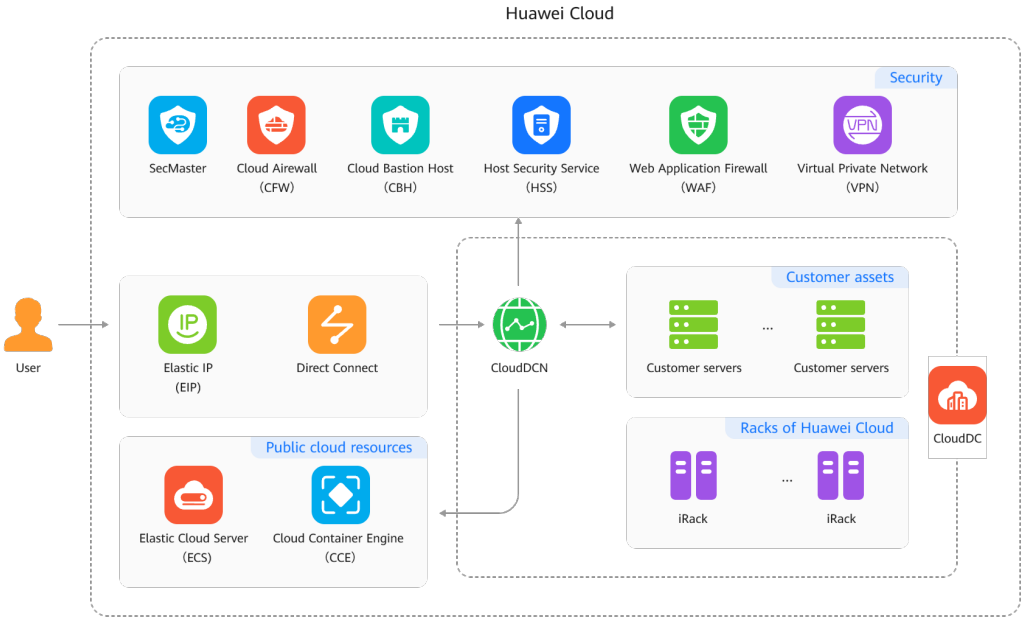
Related Services

- Cloud Container Engine (CCE)
- Ubiquitous Cloud Native Service (UCS)

3.3 Going Global

Scenario

You can deploy your assets in global data centers to rapidly establish IT infrastructure capabilities worldwide.



Benefits

- Wide coverage: Data centers are accessible in more than 23 AZs, spanning over 14 countries and regions. You can directly purchase and use the services in these data centers without having to select locations and build infrastructure.
- High reliability: Data centers feature multi-AZ high reliability and comply with related regulations. This helps you meet the requirements of industry standards and regulations.
- Robust security: With Huawei Cloud's "1+7" defense system, globally distributed sites can enjoy the same level of protection as large data centers.

Key Components

- iRack provides air-cooled intelligent racks.
- Equipment room services (deterministic O&M) include consulting, deployment, and managed O&M for going global.
- Data Center O&M Service (DCOS) centrally manages globally distributed sites and provides O&M along with service ticket support.

Related Services

- SecMaster
- Cloud Firewall (CFW)
- Cloud Bastion Host (CBH)
- Host Security Service (HSS)

- Web Application Firewall (WAF)
- Virtual Private Network (VPN)

4 Instance Specifications

4.1 iRack

CloudDC provides different iRack specifications for different service scenarios.

Table 4-1 Rack specifications

Specifications	General-purpose Computing
Rack dimensions (W x D x H)	600 mm (width) x 1,200 mm (depth) x 2,200 mm (height)
Rack Height	47 U
Rated power	8 kW
Cooling	Air-cooled racks

4.2 CloudDCN

CloudDC provides CloudDCN for different service scenarios.

Table 4-2 Supported network specifications

Network Parameter	General CloudDCN
Network interface specifications	25G

5 Security

5.1 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 5-1**.

- **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 5-1 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 5-1**, customers can select different cloud service types (such as IaaS, PaaS, and SaaS services) 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 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.

5.2 Identity and Access Management

IAM Identity Authentication

Identity and Access Management (IAM) enables you to easily manage users and control their access to Huawei Cloud services and resources.

You can use Identity and Access Management (IAM) to control access to your CloudDC resources. IAM permissions define which actions are allowed or denied on your cloud resources.

After creating an IAM user, the administrator needs to add it to a user group and grant the permissions required by CloudDC to the user group. Then, all users in this group automatically inherit those permissions.

- For details about IAM, see **IAM Functions**.
- For details about the permissions required by CloudDC, see **Permissions**.

Access Control

CloudDC uses network ACLs to protect the entire CloudDCN subnet. A network ACL is an optional layer of security for your subnets. You can associate one or more subnets with a network ACL to control traffic in and out of the subnets.

You can create, view, modify, delete, enable, disable network ACLs, associate subnets with or disassociate them from network ACLs, add and modify ACL rules, change the sequence of ACL rules, enable, disable, and delete ACL rules.

You can define network ACL rules to control traffic in and out of the subnets.

5.3 Auditing and Logging

Auditing

Cloud Trace Service (CTS) records operations on cloud resources in your account. You can use the logs to perform security analysis, track resource changes, audit compliance, and locate faults.

After CTS is enabled, it can record CloudDC operations.

- If you want to enable and configure CTS, refer to **Cloud Trace Service Getting Started**.
- The CloudDC operations that can be recorded by CTS are listed in **Table 5-1**.

Table 5-1 CloudDC operations recorded by CTS

Service	Operation	Resource Type
CTS	Updating an intelligent rack	Intelligent rack

Service	Operation	Resource Type
CTS	Creating a tag for an intelligent rack	Intelligent rack
CTS	Deleting a tag from an intelligent rack	Intelligent racks
CTS	Modifying the IDC description of an equipment room	-
CTS	Creating a private image	-
CTS	Modifying image information	-
CTS	Deleting an image	-
CTS	Installing the OS on an iMetal server	iMetal server
CTS	Changing the OS of an iMetal server	iMetal server
CTS	Uninstalling the OS of an iMetal server	iMetal server
CTS	Creating a tag for an iMetal server	iMetal server
CTS	Deleting a tag from an iMetal server	iMetal server
CTS	Changing the IP address of an iMetal server	iMetal server
CTS	Exporting logs	iMetal server
CTS	Resetting a password	iMetal server
CTS	Ordering an iMetal server	iMetal server
CTS	Stopping, starting, and restarting an iMetal server	iMetal server

Logs

BMC events and alarms of iMetal servers to can be reported to the CloudDC console. You can export the BMC logs of iMetal servers via the CloudDC console for routine O&M and fault diagnosis of the servers.

For details about how to export iMetal server logs, see **Exporting iMetal Server Logs**.

6 Notes and Constraints

Constraints on Using iRack

- Transmission devices, such as your own WDM devices, cannot be deployed in CloudDC.
- Only devices with dual power supplies or converters can be deployed.
- The bare metal servers to be managed in CloudDC must have at least a one-year hardware warranty.

Constraints on Using iMetal

- External hardware devices (such as USB devices, bank USB keys, external hard disks, and dongles) cannot be loaded.
- Only devices from specified vendors can be deployed.
- Do not upgrade the OS kernel, or the hardware driver may become incompatible with the iMetal server and adversely affect the server reliability.

7 CloudDC and Other Services

Figure 7-1 shows the relationships between CloudDC and other services. Table 7-1 lists the interactive services and related features.

Figure 7-1 Relationships between CloudDC and other services

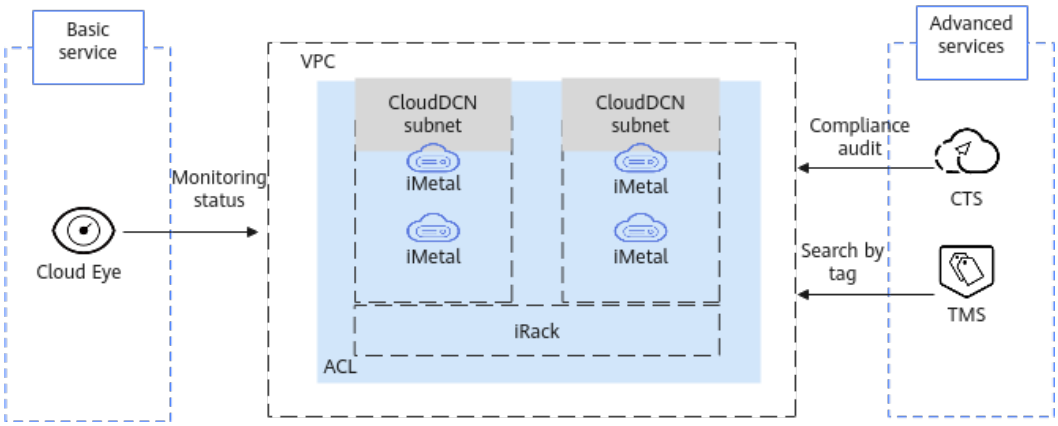


Table 7-1 Relationships between CloudDC and other services

Service Name	Interaction with CloudDC	Related Feature
Virtual Private Cloud (VPC)	VPC provides a dedicated logically isolated network for iMetal servers. You can easily configure and manage the networks in a VPC, and make changes to these networks as needed, quickly and securely. In addition, you can use network ACLs to control access rules to enhance the security of the iMetal server.	Creating a network ACL Creating a CloudDCN subnet
Cloud Eye	After purchasing an iMetal server, you can view the server status.	Monitoring an iMetal server
Log Tank Service (LTS)	Records iMetal-related operations for later query, audit, and backtrack.	Key operations supported by CTS
Tag Management Service (TMS)	Identifies iMetal servers for easy classification and search.	Adding a tag Searching for resources by tag

8 Permissions

If you need to grant your enterprise personnel permission to access your CloudDC resources, use Identity and Access Management (IAM). IAM provides identity authentication, fine-grained permissions management, and access control. IAM helps you securely access your Huawei Cloud resources.

With IAM, you can create IAM users and grant them permission to access only specific resources.

If your Huawei Cloud account 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**.

CloudDC Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and then 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.

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

You can grant permissions by using policies.

Policies: A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access.

Table 8-1 lists all the system-defined permissions for CloudDC.

Table 8-1 System-defined permissions for CloudDC

Policy Name	Description	Type	Dependencies
CloudDC FullAccess	Full permissions for CloudDC.	System-defined policies	None

Helpful Links

- IAM Service Overview
- Creating an IAM User and Granting CloudDC Permissions

9 Region and AZ

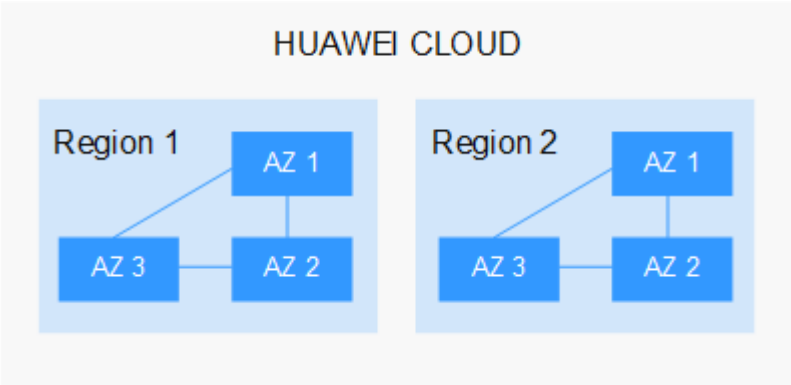
Concept

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 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**.

