Cloud Phone Host

Service Overview

Issue 01

Date 2024-12-05

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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.

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 Phone Host?

Overview

Cloud Phone Host (CPH) provides you with cloud phones virtualized from Kunpeng Bare Metal Servers (BMSs) of Huawei Cloud. These virtual phones run native Android. You can remotely control a cloud phone in real time to run Android applications on the cloud, or use the computing power of cloud phones to build applications for scenarios like cloud gaming, virtual office, and live streaming.

Why CPH?

CPH extends functions of mobile phones and can be used in scenarios such as application simulation tests, cloud mobile gaming, live streaming interaction, and virtual office, so that mobile applications can also run intelligently on the cloud.

- Lower Costs, Higher Efficiency

  In Internet industry scenarios such as application simulation tests, the processing efficiency of a single mobile phone is limited. However, by using cloud phones, you can significantly improve the processing efficiency and reduce the cost of manual operations and equipment procurement and maintenance.

- Security Assurance

  CPH runs application data on the cloud and provides more secure and efficient mobile office solutions for industries that have high requirements on information security, such as government and finance. Employees can log in to the office system from their cloud phones. Public and private data is stored separately. Enterprises can intelligently manage cloud phone servers, reducing costs and improving efficiency while ensuring information security.

- Exploring New Possibilities in the Gaming and Live Streaming Industries

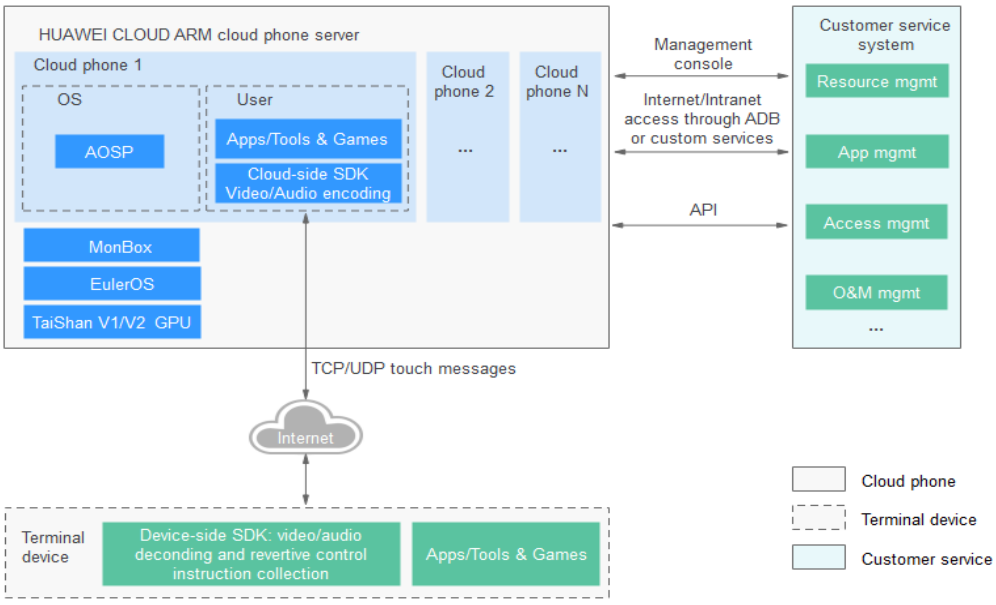
  CPH provides new interactive experience for industries such as gaming and live streaming. It helps explore new business models and market space. For example, in the cloud mobile gaming scenario, a game runs on a virtual phone on the cloud. It can be installed and deployed before play and can be dynamically loaded during play. In this way, end players play games without downloading them. This greatly improves the player conversion rate. In addition, users with medium or low mobile phone configurations can run large-scale mobile games smoothly, which expands the user scope of games.

For more innovative technologies and advantages of CPH, see **CPH Advantages**.

Product Architecture

The CPH architecture consists of three parts: cloud phone, terminal device, and customer service.

Figure 1-1 CPH architecture



Based on Huawei TaiShan Arm servers, CPH integrates multiple highly cost-effective GPUs to provide professional graphics processing capabilities. The TaiShan server runs EulerOS as the host OS. The host OS uses the in-house MonBox technology to generate a container, and the Android Open Source Project (AOSP) system runs in the container to virtualize multiple cloud phones. Both the TaiShan server and CPH system use the Arm architecture, so translation compute power loss caused by instruction set conversion is reduced, and better user experience is delivered.

CPH provides video, audio, and touch SDKs. You can develop terminal-based applications to obtain audios and videos of cloud phones. Another option is to gather touch instructions, such as tapping, swiping, or clicking, and execute them on cloud phones.

On the service side, you can use the management console, APIs, Android Debug Bridge (ADB) ports, and other customized ports to manage resources, applications, O&M, and access of cloud phone servers.

- Resource management: Purchase and query cloud phone servers.
- Application management: Push, install, and uninstall cloud phone applications.
- O&M management: Restart, reset, stop, and start cloud phone servers.
- Access management: cloud phone server access authentication

Available Regions

CPH is only available in the following regions:

- CN East-Shanghai1
- CN East-Shanghai2
- CN South-Guangzhou
- CN Southwest-Guiyang1
- CN-Hong Kong
- AP-Singapore
- LA-Santiago

Target Users

CPH is mainly used by enterprise users. Users should have basic computer knowledge and certain development capabilities to perform secondary development based on cloud phones. If you (individual customer) want to try out or perform some simple operations, you can also purchase a cloud phone. We will provide related operation guide and expert assistance.

How to Use

You can access CPH through a web-based management console or by calling HTTPS-based APIs.

- Calling APIs

  To integrate CPH into your system for secondary development, use APIs to access CPH. For details, see the **API Reference**.

- Through the management console

  To perform other operations, such as purchasing and connecting to a cloud phone, log in to the management console to access CPH.

  You obtain cloud phones only after purchasing a server. To purchase a server and obtain the corresponding number of cloud phones, you only need to specify the server type, instance specifications, phone image, and required network configuration. For details about how to purchase and use a cloud phone, see **Buying a Cloud Phone Server**.

2 CPH Advantages

CPH relies on Huawei Cloud servers, innovative technologies, and peripheral services to enable mobile applications to run on the cloud. Compared with common mobile phone simulation solutions, CPH has outstanding performance, compatibility, and stability.

First in the Industry

It is the first Arm-based CPH solution in the public cloud industry. Both terminal devices and CPH have Arm inside. Native applications require no instruction set translation. Cloud phone applications are highly compatible, and their operating performance can be improved by up to 80% compared with the x86 emulator solution. Also, professional GPU acceleration is available to run large-scale games without pressure.

Enhanced Security

Depending on the clustered deployment and operation capabilities of Huawei Cloud, CPH seamlessly interconnects with multiple public cloud services, supports user data mounting within seconds and data persistence. It processes data on the cloud, which is more secure and more powerful to handle enterprise-level large-scale applications.

Cloud-based upgrades will make CPH always stand out among its peers while eliminating depreciation cost.

High Flexibility

Cloud phones can be customized as needed and be purchased on demand to better handle uncertain enterprise service developments. Cloud phones can be provisioned in batches. You can manage them with ease. For instance, you can batch restart, reset, power on, or power off them.

Upgraded Security

CPH service data is stored on the cloud instead of being on premises. It is secure with protection from security services including Anti-DDoS and Situation Awareness.

Comparison Between CPH and Other Mobile Phone Simulation Solutions

Common mobile phone simulation solutions in the market include the x86 emulator solution and mobile phone teamwork control solution. **Table 2-1** lists the advantages and disadvantages of the three solutions.

Table 2-1 Comparison between CPH and other mobile phone simulation solutions

Dimension	x86 Emulator	Physical Phone	Cloud Phone of Huawei
Performance	Poor Conversion between x86 and Arm instruction sets is required, resulting in low efficiency and at least 50% performance loss.	Medium Cannot exceed the performance of a mobile phone.	High CPH is based on Arm servers and offers various performance and storage specifications. It is far more powerful than physical mobile phones.
Compatibility	Poor Complex x86 instructions are not converted into simplified Arm instructions in one-to-one mode, causing severe application compatibility issues. These issues persist for a long time and are difficult to resolve.	High Same as mobile phones, ensuring application compatibility.	High High compatibility of Arm-based native applications
Stability	Medium The stability is hard to ensure because it is implemented based on various external open-source or non-commercial simulator software.	Extremely poor A large number of second-hand mobile phones are non-server products. In addition, manual soldering points and complex cable connections cannot ensure product quality and stability.	High In-house high-performance Arm chips and Arm servers have been widely used in the market, providing high stability and reliability.

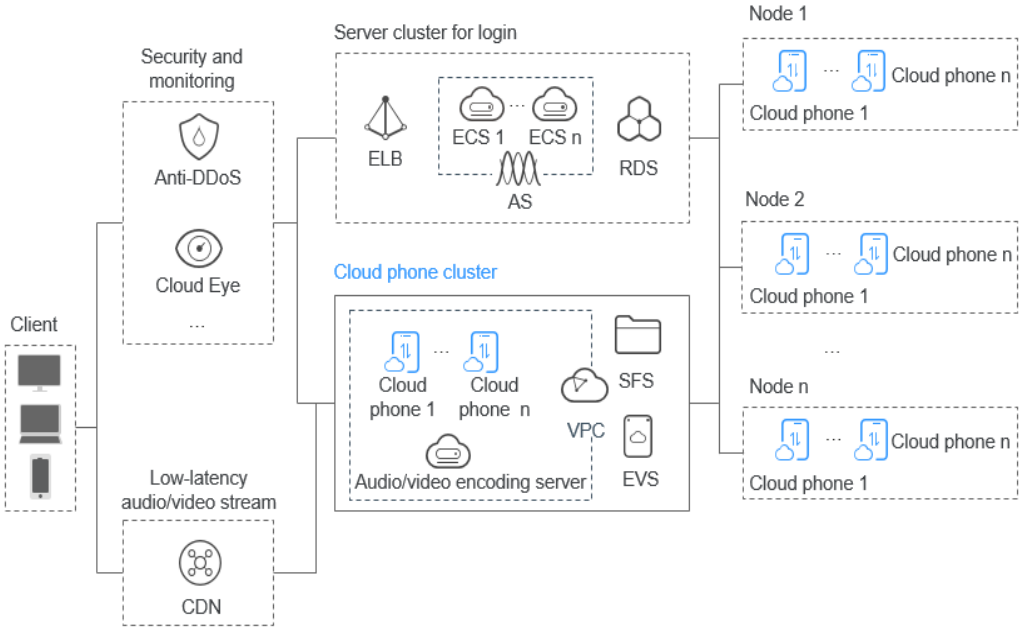
Dimension	x86 Emulator	Physical Phone	Cloud Phone of Huawei
Availability	High x86 servers and emulator software are used to build the system, which has low requirements and high resource availability.	Extremely poor It is very difficult to obtain sufficient and stable sources of mobile phones. The second-hand mobile phone market is changing rapidly, and the availability of the target mobile phones in the market is extremely poor.	High The product is provided as a public cloud service, which features large volume, flexible usage, and high elasticity of resources. The resources can be charged by month.
Simulation	Poor Based on the software upper-layer technology, many mobile phone parameters can be modified, the features are obvious, but the x86 emulator is easily detected by the upper-layer application as a simulator.	High Exactly mobile phone used.	High Fully simulate mobile phones. If the cost-effective AOSP mode is used, underlying hardware data can be simulated for applications.
Specifications Flexibility	High Specifications can be set flexibly.	Poor Devices are purchased based on the set specifications, which are not flexible.	High The specifications can be flexibly set and adjusted, and high-specification overcommitment instances can be easily implemented.

3 Scenarios

Cloud Gaming

Cloud gaming is a popular trend of the game industry. It provides players with a download-free game service that is independent of mobile phone performance. The video streaming modes it uses include PC game streaming and mobile game streaming. As a cloud-based emulation phone, a cloud phone server can take the advantage of instruction isomorphism of mobile games and carry game applications on the cloud.

Figure 3-1 Cloud gaming architecture



Architecture description:

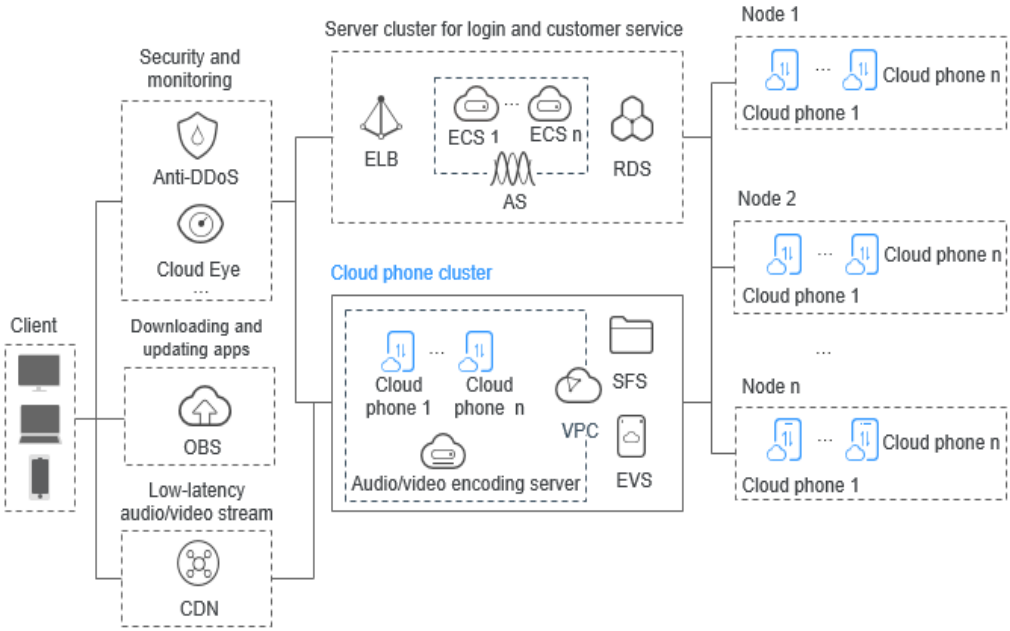
- Mobile game applications are installed on cloud phones. After being streaming processed and encoded, the audio and video images on the cloud phones are sent to clients for display. The cloud phones receive operation instructions from the client to control games on the cloud phones.

- The login server cluster uses Elastic Load Balance (ELB) and Auto Scaling (AS) to handle ultra-large concurrent data requests.
- Cloud phones can be deployed on central and edge nodes to effectively reduce the user interaction latency and achieve optimal experience and best bandwidth cost-effectiveness.

Mobile Office

With the popularization of mobile apps, more and more enterprises are starting to allow work from mobile terminals. However, they are faced with the challenge of data security. Although purchasing customized secure mobile phones can enhance security, leakage of sensitive data cannot be prevented. As an alternative solution, cloud phones store core enterprise data on the cloud and control access to mobile phone screens only within authorized employees.

Figure 3-2 Mobile office architecture



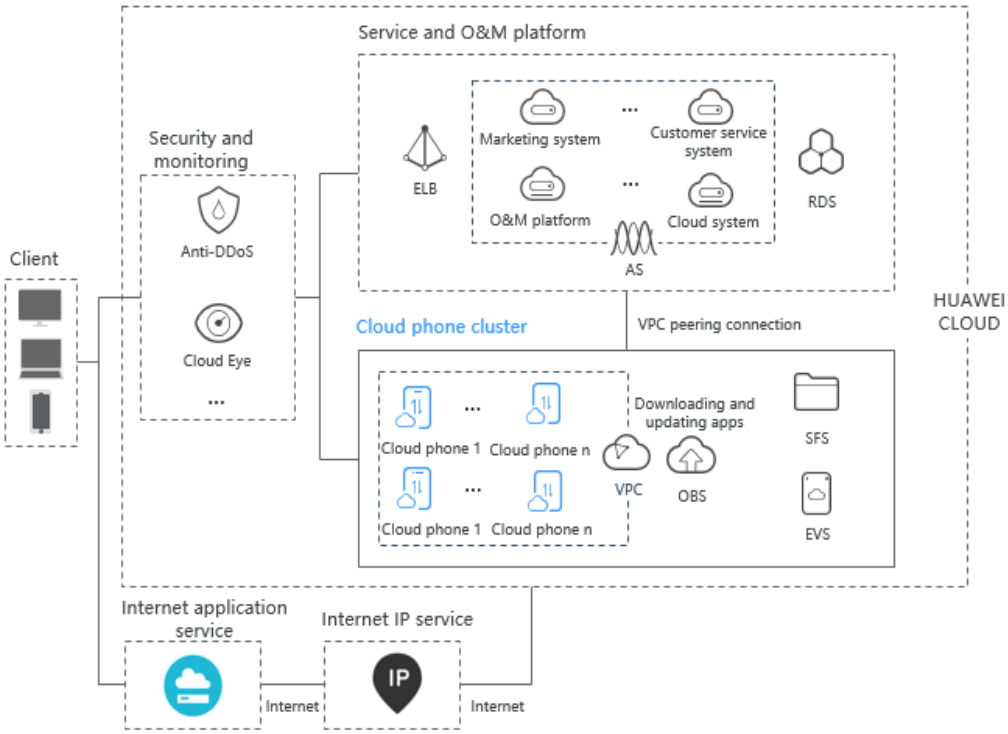
Architecture description:

- After enterprise applications are uploaded to Object Storage Service (OBS), they are installed on cloud phones in batches. Audio and video images on cloud phones are streamed and encoded and then sent to clients for display. In addition, the cloud phones receive operation instructions from clients to control the applications on cloud phones. Enterprise data is stored on the cloud, which is more secure and reliable.
- The server cluster for login or customer service uses ELB and AS to handle ultra-large-scale concurrent data requests.
- Cloud phones can be deployed on central and edge nodes to effectively reduce the user interaction latency and achieve optimal experience and best bandwidth cost-effectiveness.

Application Simulation Testing

Generally, mobile phones provide services for individuals. As the type and number of mobile applications increase, enterprises may need to run a large number of mobile applications on mobile phones in specific scenarios to implement automation or intelligence functions. To run these applications, a large number of simulation mobile phones are needed.

Figure 3-3 Application simulation test architecture



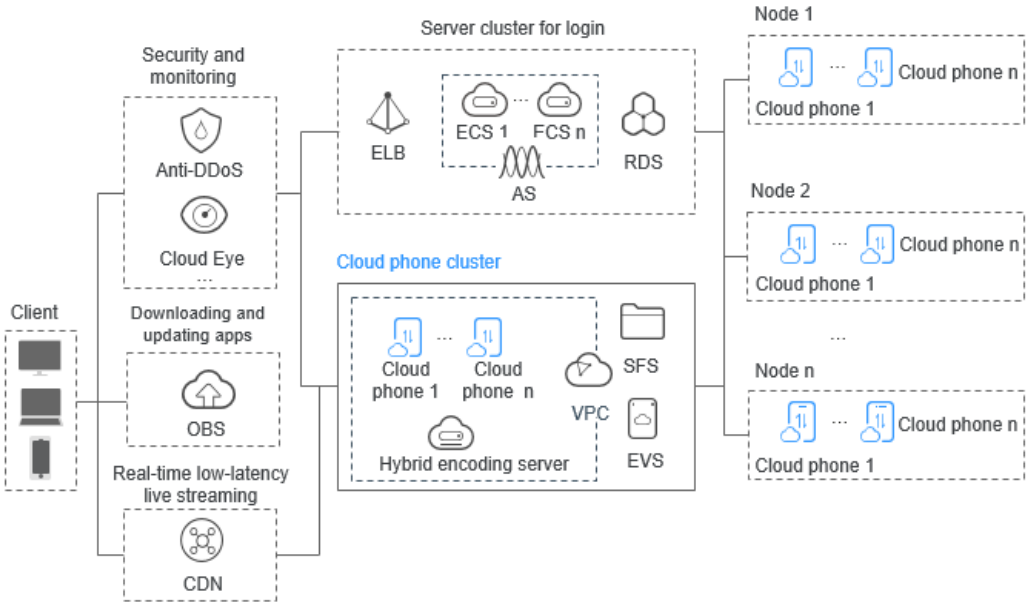
Architecture description:

- Mobile applications are installed on cloud phones. Enterprise orchestrated scripts control cloud phones to run one or more apps. Personalized script operations are able to handle various scenarios.
- An enterprise can build its own cloud phone management and O&M platform, marketing system, or automation script platform on an ECS and use two independent VPCs to control the platforms separately.
- Cloud phone applications can be centrally stored in OBS buckets, reducing network bandwidth consumed by installing or updating these applications.
- A wide range of security and monitoring services ensure that applications are not interrupted by online threats.

Streaming Interaction

Streaming interaction is another CPH scenario. It allows the host to stream the mobile phone screen to audiences and interact with them to bring an enjoyable interaction experience.

Figure 3-4 Streaming interaction architecture



Architecture description:

- Mobile phone applications and game applications are installed on cloud phones. These applications output one or combine more mobile phone screens to the encoding server for integrated encoding. Then, the screens are copied and pushed to different clients (such as PCs, mobile phones, and tablets) for display. Cloud phones receive operation instructions from one or more clients.
- The login server cluster uses ELB and AS to handle ultra-large concurrent data requests.

4 Servers for General-Purpose Cloud Phones

Overview

Servers for general-purpose cloud phones provide software-defined mobile phone capabilities and emulate key hardware and software of mobile phones, such as sensors and networks. They are applicable to automatic application tests and mobile office.

Cloud Phone Server Specifications

Table 4-1 Server specifications

Flavor	Configuration
physical.rx1.xlarge	• CPU: Hi1616 (2 x 32 cores, 2.4 GHz) • Memory: 256 GB DDR4 RAM • Local disk: 2 x 1.2 TB SAS + 800 GB SSD • NIC: 2 x 10GE • GPU: 3 x WX5100
physical.kg1.4xlarge.cp	• CPU: Kunpeng 920 (2 x 64 cores, 2.6 GHz) • Memory: 512 GB DDR4 RAM • Local disk: N/A • NIC: 2 x 10GE • GPU: 5 x WX5100
physical.rx2.32xlarge.4	• CPU: Kunpeng 920 (2 x 64 cores, 2.6 GHz) • Memory: 512 GB DDR4 RAM • Local disk: N/A • NIC: 2 x 10GE • GPU: 5 x WX5100

Flavor	Configuration
physical.rx3.32xlarge.4	• CPU: Kunpeng 920 (2 x 64 cores, 2.6 GHz) • Memory: 512 GB DDR4 RAM • Local disk: N/A • NIC: 2 x 25GE • GPU: 2 x W6800

Supported Cloud Phone Specifications

Table 4-2 Specifications of cloud phones that can be virtualized from a physical.rx1.xlarge server

Flavor	Configuration
rc1.se	• vCPUs and memory: 4 vCPUs | 8 GB • Screen resolution: 1280x720 • DPI: 320 • Rendering frame rate (fps): 30 • Quantity: 60
rc1.plus	• vCPUs and memory: 6 vCPUs | 12 GB • Screen resolution: 1280x720 • DPI: 320 • Rendering frame rate (fps): 60 • Quantity: 30
rx1.cp.c60.d32.e1v1.qemu	• vCPUs and memory: 2 vCPUs | 3 GB | 32 GB • Screen resolution: 960x540 • Quantity: 60 • EIP/VIP: 1/1

Table 4-3 Specifications of cloud phones that can be virtualized from a physical.kg1.4xlarge.cp or physical.rx2.32xlarge.4 server

Flavor	Configuration
rc2.se	• vCPUs and memory: 5 vCPUs | 10 GB • Screen resolution: 1280x720 • DPI: 320 • Rendering frame rate (fps): 30 • Quantity: 100

Flavor	Configuration
rc2.plus	• vCPUs and memory: 6 vCPUs | 12 GB • Screen resolution: 1280x720 • DPI: 320 • Rendering frame rate (fps): 30 • Quantity: 80
rc2.pro	• vCPUs and memory: 8 vCPUs | 16 GB • Screen resolution: 1280x720 • DPI: 320 • Rendering frame rate (fps): 60 • Quantity: 60
rc2.max	• vCPUs and memory: 16 vCPUs | 24 GB • Screen resolution: 1920x1080 • DPI: 440 • Rendering frame rate (fps): 30 • Quantity: 40
rc2.pro_max	• vCPUs and memory: 20 vCPUs | 32 GB • Screen resolution: 1920x1080 • DPI: 440 • Rendering frame rate (fps): 30 • Quantity: 20

Table 4-4 Specifications of cloud phones that can be virtualized from a physical.rx3.32xlarge.4 server

Flavor	Configuration
rc3.se	• vCPUs and memory: 5 vCPUs | 10 GB • Screen resolution: 1280x720 • DPI: 320 • Rendering frame rate (fps): 30 • Quantity: 100
rc3.plus	• vCPUs and memory: 6 vCPUs | 12 GB • Screen resolution: 1280x720 • DPI: 320 • Rendering frame rate (fps): 60 • Quantity: 90

Flavor	Configuration
rc3.pro	• vCPUs and memory: 8 vCPUs | 16 GB • Screen resolution: 1920x1080 • DPI: 440 • Rendering frame rate (fps): 60 • Quantity: 60
rc3.max	• vCPUs and memory: 16 vCPUs | 24 GB • Screen resolution: 1920x1080 • DPI: 440 • Rendering frame rate (fps): 60 • Quantity: 40
rc3.pro_max	• vCPUs and memory: 20 vCPUs | 32 GB • Screen resolution: 1920x1080 • DPI: 440 • Rendering frame rate (fps): 60 • Quantity: 20

- **Quantity**: indicates the number of cloud phones that can be virtualized from a server. For example, if **Quantity** is **60**, you can have 60 cloud phones virtualized from a server.
- You can customize the disk size and network settings when purchasing a server.

Cloud Phone 2.0

CPH has released cloud phone 2.0 specifications that decouple storage from network. You are advised to buy cloud phone 2.0 instead of cloud phone 1.0 and select the 2.0 specifications corresponding to the 1.0 specifications in the following table.

Cloud Phone 2.0 Specifications	Quantity	Cloud Phone 1.0 Specifications	Server Specifications
rc1.plus	30	rx1.cp.c15.d46.e1v1	physical.rx1.xlarge physical.rx1.xlarge.cg
		rx1.cp.c30.d23.e1v1	physical.rx1.xlarge
		rx1.cp.c30.d23.e5v5	physical.rx1.xlarge
		rx1.cp.dedicated.c30.d25.e3v3	physical.rx1.xlarge.dedicated

rc1.se	60	rx1.cp.c45.d15.e1v1	physical.rx1.xlarge
		rx1.cp.dedicated.c45.d10.e1v1.a250	physical.rx1.xlarge.dedicated
		rx1.cp.c60.d10.e0v1	physical.rx1.xlarge
		rx1.cp.c60.d10.e0v60	physical.rx1.xlarge
		rx1.cp.c60.d10.e1v1	physical.rx1.xlarge
		rx1.cp.c60.d8.e1v1.a200	physical.rx1.xlarge
		rx1.cp.dedicated.c60.d16.e1v1	physical.rx1.xlarge.dedicated
		rx1.cp.dedicated.c60.d18.e1v1	physical.rx1.xlarge.dedicated
		rx1.cp.dedicated.c60.d18.e5v5	physical.rx1.xlarge.dedicated
		rx1.cp.dedicated.c60.d8.e1v1.a200	physical.rx1.xlarge.dedicated
		rx1.cp.vp.c60.d10.e1v1	physical.rx1.xlarge
rs1.se	75	rx1.cp.c75.d11.e5v5.br75	physical.rx1.xlarge
		rx1.cp.c75.d15.e1v1	physical.rx1.xlarge
		rx1.cp.dedicated.c75.d11.e1v1	physical.rx1.xlarge.dedicated
		rx1.cp.dedicated.c75.d15.e1v1	physical.rx1.xlarge.dedicated
		rx1.cp.dedicated.c75.d15.e5v5	physical.rx1.xlarge.dedicated
		rx1.cp.dedicated.c75.d6.e1v1.a200	physical.rx1.xlarge.dedicated
		rx1.cp.c90.d6.e1v1	physical.rx1.xlarge
rc2.max	40	kg1.cg.c20.d30SSD.e1v1	physical.kg1.4xlarge.cg
		kg1.cg.c20.d50SSD.e1v1	physical.kg1.4xlarge.cg
		kg1.cg.c20.d50SSD.e1v1.s400	physical.kg1.4xlarge.cg
		kg1.cp.c20.d64SSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cg.c30.d50SSD.e1v1	physical.kg1.4xlarge.cg
		kg1.cp.c31.d20SSD.e3v3	physical.kg1.4xlarge.cp
		kg1.cp.c31.d32GPSSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.c31.fd32GPSSD.e3v3	physical.kg1.4xlarge.cp

		kg1.cp.dedicated.c31.d100GPSSD.e1v1.a4096	physical.kg1.4xlarge.cp.dedicated
		R2c.xlarge.4	physical.kg1.4xlarge.cp
		kg1.cg.c40.d30SSD.e1v1	physical.kg1.4xlarge.cg
		kg1.cg.c40.d30SSD.e1v1.a200	physical.kg1.4xlarge.cg
		kg1.cp.c40.d32GPSSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cg.c48.d500SSD.e1v1.s500	physical.kg1.4xlarge.cg
rc2.pro	60	kg1.cg.c60.d30SSD.e1v1.s800	physical.kg1.4xlarge.cg
		kg1.cg.c60.d50SSD.e1v1	physical.kg1.4xlarge.cg
		kg1.cp.c60.d10GPSSD.e1v1.a300	physical.kg1.4xlarge.cp
		kg1.cp.c60.d16GPSSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.c60.d16SSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.c60.d32GPSSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.c60.d32SSD.e5v5	physical.kg1.4xlarge.cp
		kg1.cp.c60.d64GPSSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.c60.d64SSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.c60.fd20GPSSD.e5v5	physical.kg1.4xlarge.cp
		kg1.cp.dedicated.c60.fd30GPSSD.e1v1.a700	physical.kg1.4xlarge.cp.dedicated
		R2s.xlarge.2	physical.kg1.4xlarge.cp
rc2.plus	80	kg1.cp.c80.d30GPSSD.e1v1	physical.kg1.4xlarge.cp
rc2.se	100	kg1.cp.c90.d14.e1v1	physical.kg1.4xlarge.a.cp
		kg1.cp.c100.d10GPSSD.e0v100	physical.kg1.4xlarge.cp
		kg1.cp.c100.d10GPSSD.e100v100	physical.kg1.4xlarge.cp
		kg1.cp.c100.d10GPSSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.c100.d10SSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.c100.d16GPSSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.c100.d16SSD.e0v100	physical.kg1.4xlarge.cp
		kg1.cp.c100.d16SSD.e0v20	physical.kg1.4xlarge.cp
		kg1.cp.c100.d16SSD.e10v10	physical.kg1.4xlarge.cp
		kg1.cp.c100.d16SSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.c100.d32SSD.e1v1	physical.kg1.4xlarge.cp

		kg1.cp.c100.fd16GPSSD.e10v10	physical.kg1.4xlarge.cp
		kg1.cp.c100.fd24GPSSD.e0v1	physical.kg1.4xlarge.cp
		kg1.cp.dedicated.c100.d10GPSSD.e1v1.a1024	physical.kg1.4xlarge.cp.dedicated
		rx2.cp.dedicated.c100.d45GPSSD.e1v1	physical.rx2.32xlarge.4.dedicated
rs2.plus	124	kg1.cp.c120.d10GPSSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.c120.d10SSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.c120.d16GPSSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.c120.fd16GPSSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.c120.fd16GPSSD.e2v2	physical.kg1.4xlarge.cp
		kg1.cp.c130.d10GPSSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.dedicated.c120.fd10GPSSD.e1v1	physical.kg1.4xlarge.cp.dedicated
		kg1.cp.dedicated.c120.fd18GPSSD.e1v1	physical.kg1.4xlarge.cp.dedicated
rs2.se	150	kg1.cp.c150.d10GPSSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.c150.fd10GPSSD.e0v1	physical.kg1.4xlarge.cp
		kg1.cp.c150.fd10GPSSD.e1v1	physical.kg1.4xlarge.cp
		kg1.cp.c150.fd10GPSSD.e2v2	physical.kg1.4xlarge.cp
		kg1.cp.c150.fd15GPSSD.e10v10	physical.kg1.4xlarge.cp
		kg1.cp.dedicated.c150.d10GPSSD.e1v1.a1024	physical.kg1.4xlarge.cp.dedicated
		kg1.cp.dedicated.c150.d8GPSSD.e1v1.a500	physical.kg1.4xlarge.cp.dedicated
		kg1.cp.dedicated.c150.fd10GPSSD.e1v1	physical.kg1.4xlarge.cp.dedicated
		rx2.cp.dedicated.c150.d30GPSSD.e1v1	physical.rx2.32xlarge.4.dedicated
		rx2.cp.dedicated.c150.d8GPSSD.e1v1	physical.rx2.32xlarge.4.dedicated
		rx2.cp.dedicated.c150.d8GPSSD.e1v1.a500	physical.rx2.32xlarge.4.dedicated
rs2a.pro	72	kg1.cp.c72.d10.e1v1	physical.kg1.4xlarge.a.cp
		kg1.cp.c72.d18.e1v1	physical.kg1.4xlarge.a.cp

rc3.pro_max	20	rx3.cp.c14.d32GPSSD.e1v1	physical.rx3.32xlarge.4
		rx3.cp.c20.d32GPSSD.e1v1	physical.rx3.32xlarge.4
rc3.max	40	rx3.cp.c30.d32GPSSD.e1v1	physical.rx3.32xlarge.4
rc3.pro	60	rx3.cp.c60.d27GPSSD.e0v60.a100	physical.rx3.32xlarge.4
rc3.plus	90	rx3.cp.c90.d16GPSSD.e1v1	physical.rx3.32xlarge.4
		rx3.cp.dedicated.c90.d16GPSSD.e1v1	physical.rx3.32xlarge.4.dedicated
rs3.plus	124	rx3.cp.c120.d10GPSSD.e0v120	physical.rx3.32xlarge.4
		rx3.cp.c120.d10GPSSD.e1v1	physical.rx3.32xlarge.4
rs3.se	150	rx3.cp.c150.d10GPSSD.e1v1	physical.rx3.32xlarge.4
		rx3.cp.c150.d10GPSSD.e1v1.a1024	physical.rx3.32xlarge.4
		rx3.cp.dedicated.c150.d30GPSSD.e10v10	physical.rx3.32xlarge.4.dedicated
		rx3.cp.dedicated.c150.d30GPSSD.e1v1	physical.rx3.32xlarge.4.dedicated
		rx3.cp.dedicated.c150.d8GPSSD.e1v1.a3400	physical.rx3.32xlarge.4.dedicated
		rx3.cp.dedicated.c150.d8GPSSD.e1v1.a500	physical.rx3.32xlarge.4.dedicated
		rx3.cp.sp.c150.d10GPSSD.e1v1	physical.rx3.32xlarge.4

5 Cloud Mobile Gaming Servers

Overview

Cloud mobile gaming servers use GPU hardware acceleration and graphics interfaces to run mobile games on the cloud. They are ideal for promoting mobile game trial and running mobile games on the cloud.

Cloud mobile gaming servers use two types of CPUs: Hi1616 and Kunpeng 920. Kunpeng 920 provides powerful computing power that is 2.9 times higher than the previous generation and high-performance networks.

Specifications

Table 5-1 Server specifications

Flavor	Configuration
physical.rx1.xlarge.cg	• CPU: Hi1616 (2 x 32 cores, 2.4 GHz) • Memory: 256 GB DDR4 RAM • Local disk: 2*1.2 TB SAS + 800 GB SAS SSD • NIC: 2 x 10GE • GPU: 3 x WX5100 • Extended configuration: cloud mobile gaming access software
physical.kg1.4xlarge.cg	• CPU: Kunpeng 920 (2 x 64 cores, 2.6 GHz) • Memory: 512 GB DDR4 RAM • Local disk: N/A • NIC: 2 x 10GE • GPU: 5 x WX5100 • Extended configuration: cloud mobile gaming access software

Supported Cloud Phone Specifications

Table 5-2 Specifications of cloud phones that can be virtualized from a physical.rx1.xlarge.cg server

Flavor	Configuration	Applicable Game
rx1.cg.c15.d30.e1v1	• Computing and storage: 2 vCPUs | 8 GB | 30 GB • Screen resolution: 1280x720 • Quantity: 15 • EIP/VIP: 1/1	• Action and shooting • Real-time strategy • Business simulation

Table 5-3 Specifications of cloud phones that can be virtualized from a physical.kg1.4xlarge.cg server

Flavor	Configuration	Applicable Game
kg1.cg.c40.d30SSD.e1v1	• Computing and storage: 2 vCPUs | 10 GB | 30 GB • Screen resolution: 1280x720 • Quantity: 40 • EIP/VIP: 1/1	• Action and shooting • Real-time strategy • Business simulation
kg1.cg.c80.d16SSD.e1v1	• Computing and storage: 2 vCPUs | 5 GB | 16 GB • Screen resolution: 960x540 • Quantity: 80 • EIP/VIP: 1/1	• Trading card • Casual and puzzle
kg1.cg.c20.d50SSD.e1v1	• Computing and storage: 6 vCPUs | 12 GB | 50 GB • Screen resolution: 1920x1080 • Quantity: 20 • EIP/VIP: 1/1	• Role-playing • Sports and racing (car racing and football) • Multiplayer

- Each field in the cloud phone specifications has a clear meaning.
  Take **rx1.cg.c15.d30.e1v1** as an example.
  rx1: indicates that the server CPU is Hi1616 (**kg1** indicates Kunpeng 920).
  cg: indicates a cloud mobile gaming server.
  c15: indicates that the cloud phone quantity is 15.

d30: indicates that the built-in storage capacity is 30 GB.

e1v1: indicates one EIP and one virtual IP address.

- **Quantity**: indicates the number of cloud phones that can be virtualized from a server. For example, if **Quantity** is **15**, you can have 15 cloud phones virtualized from a server.
- **EIPs/VIPs**: indicates the number of EIPs or VIPs bound to a server. An EIP allows a cloud phone to access the Internet. A VIP is the ingress and egress of the cloud phone traffic.

  All cloud phones share the public IP address of the same server. If **EIPs** is **0**, the cloud phone cannot access the Internet. Purchase an EIP together with a server.

EVS Disk Specifications

The physical.kg1.4xlarge.cg server does not have local disks. By default, the system purchases and attaches one or more ultra-high I/O EVS disks to provide storage space for cloud phones and implement data persistence for you.

The default capacity and number of the EVS disks purchased are related to the cloud phone specifications. For details, see **Table 5-4**.

Table 5-4 EVS disk capacity and quantity

Server Specifications	Cloud Phone Specifications	Capacity Per EVS Disk (GB)	EVS Disk Quantity
physical.kg1.4xlarge.cg	kg1.cg.c40.d30SSD.e1v1	550	3
	kg1.cg.c80.d16SSD.e1v1	550	3
	kg1.cg.c20.d50SSD.e1v1	450	3
	kg1.cg.c20.d30SSD.e1v1 (private)	300	3

NOTE

If the cloud phone specifications are marked with "private", the specifications cannot be viewed by some users.

6 Security

6.1 Shared Responsibilities

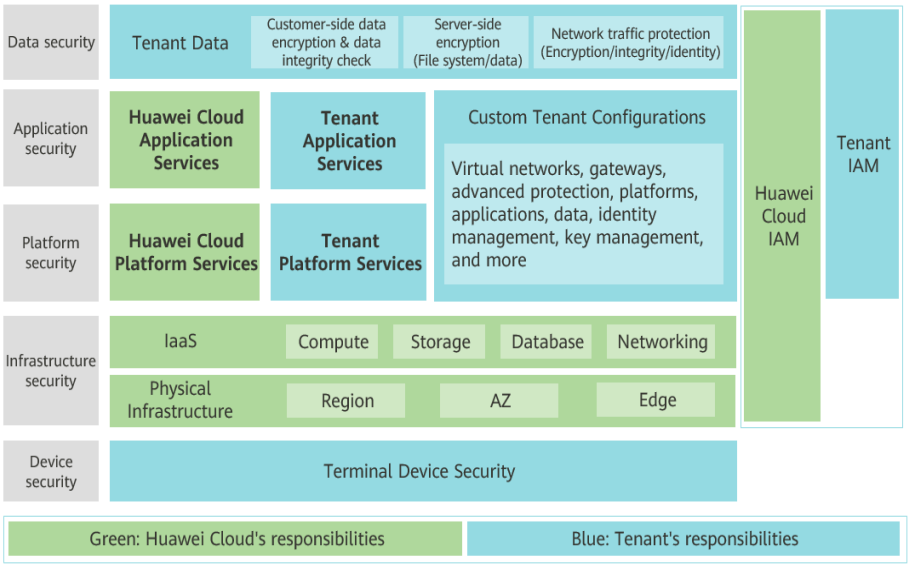
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 6-1 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 6-1 Huawei Cloud shared security responsibility model



6.2 Identity Authentication and Access Control

6.2.1 Access Control for CPH

IAM Identity Authentication

IAM provides fine-grained permissions management, user identity authentication, and resource access control.

You can use your account to create IAM users and assign permissions to the IAM users to control their access to specific resources. IAM permissions define which actions on your cloud resources are allowed or denied.

- For details about permission management, see **Permissions Management**.
- For details about how to authorize CPH, see **Creating a User and Granting CPH Permissions**.
- For details about custom policies, see **Example Permission Configuration**.
- For details about policies and supported actions, see **Permissions Policies and Supported Actions**.

Access Control

- Virtual Private Cloud (VPC)

  VPC allows you to create logically isolated virtual networks for your cloud phone servers. You can define security groups, virtual private networks (VPNs), IP address segments, and bandwidth for a VPC. This facilitates internal network configuration and management and allows you to change your network in a secure and convenient manner. You can also define rules to control access between cloud phone servers in the same security group or across different security groups to strength security.

- Security Groups

  A security group is a collection of access control rules for cloud phone servers that have the same security requirements and are mutually trusted. After a security group is created, you can add different access rules to the security group, and these rules will apply to all cloud phone servers added to this security group.

For details about how to create a VPC and security group, see **Table 2 Configuring a custom network**.

Key Pairs

A key pair, or SSH key pair, is an authentication method used when you remotely log in to Linux instances. A key pair is generated using an encryption algorithm. It contains a public key and a private key reserved for you. The public key is used to encrypt data (for example, a password), and the private key is used to decrypt the data.

Huawei Cloud stores the public key, and you need to store the private key. Do not share your private key with anyone. Keep your private key secure.

For details about how to create and use a key pair, see **Table 3 Parameters for advanced settings**.

6.3 Data Protection

CPH takes different measures to ensure data security and reliability.

- CPH is developed based on BMSs. CPH offers physical server-level performance and isolation and dedicated computing resources without any loss due to virtualization.
- CPH provides backup and restoration APIs, allowing you to back up important data to your OBS buckets (**Exporting Data from Cloud Phones in Batches**) and restore backup data from OBS buckets to specified cloud phones (**Restoring Cloud Phone Data**).
- To ensure confidentiality of your data on cloud phones, the new AOSP public image supports file-level encryption. Your data will be stored to disks in ciphertext.

6.4 Auditing and Logging

Cloud Trace Service (CTS) is a log audit service 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 CPH operations.

- For details about how to enable and configure CTS, see **CTS Getting Started**.
- For details about CPH operations that CTS can record, see **Key Cloud Phone Operations Recorded by CTS**.

- For details about how to view traces, see **Viewing Traces**.

6.5 Security Risk Monitoring

After purchasing a cloud phone server, you can view monitoring data of the server and its associated resources (such as disks and GPU cards) on Cloud Eye graphs without installing other plug-ins.

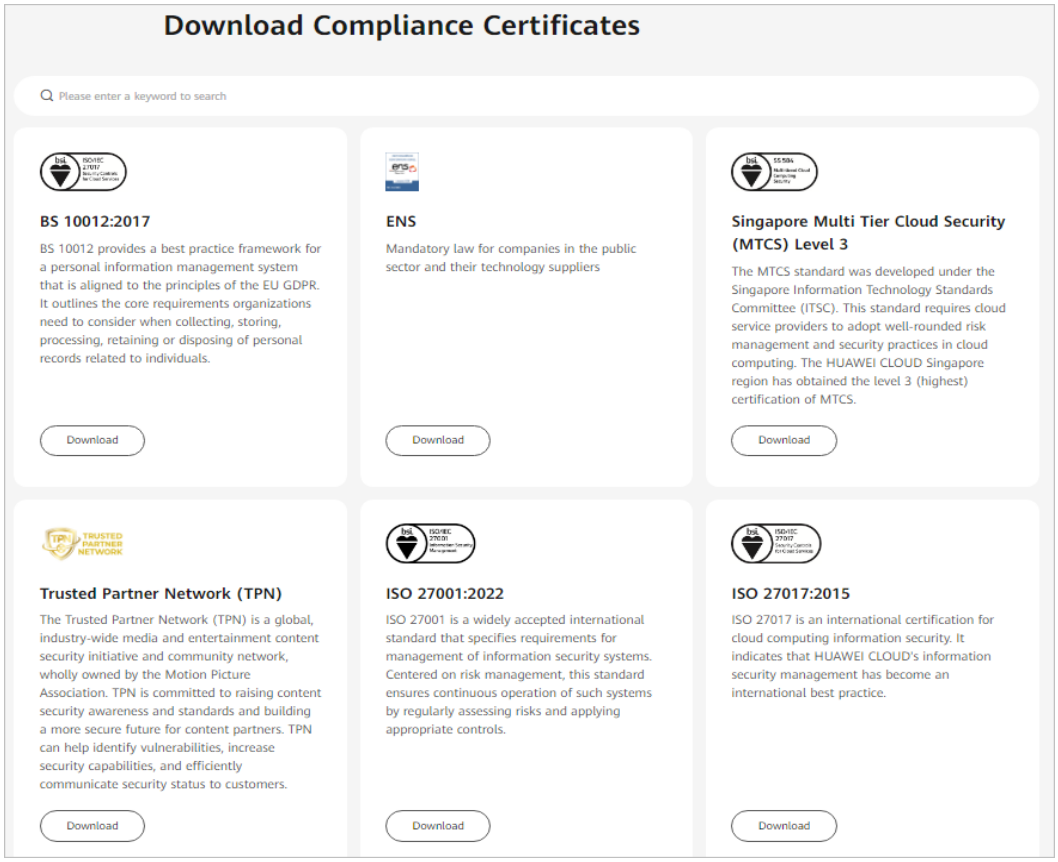
- **Supported Metrics**
- **CPH Events**
- **Viewing Metrics**
- **Creating an Alarm Rule**

6.6 Certificates

Compliance Certificates

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

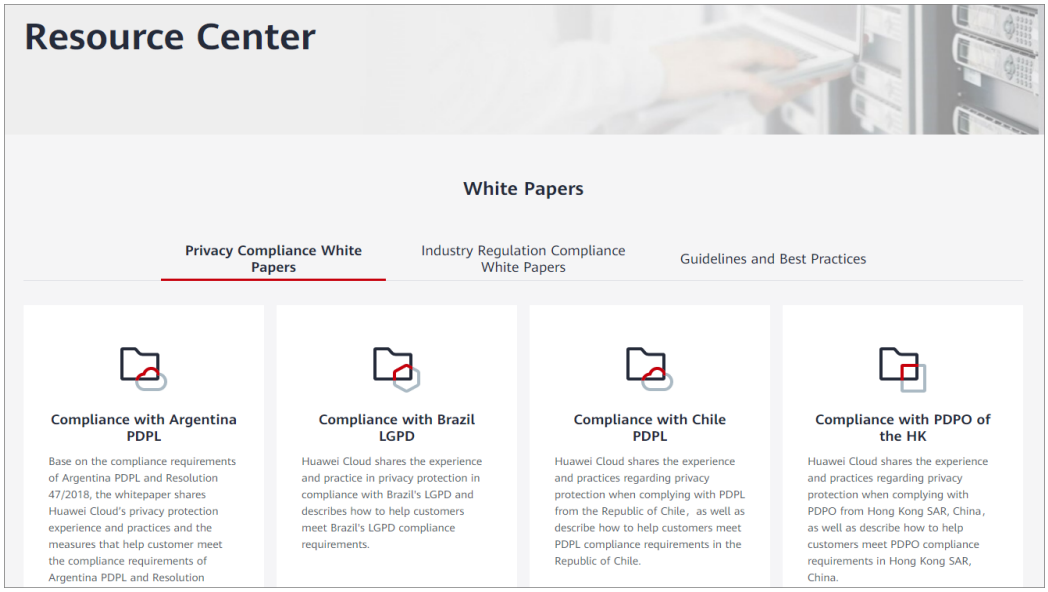
Figure 6-2 Downloading compliance certificates



Resource Center

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

Figure 6-3 Resource center



7 Billing

This topic describes CPH billing items and billing modes.

Billing Items

Figure 7-1 shows the CPH billing items.

Figure 7-1 Billing items

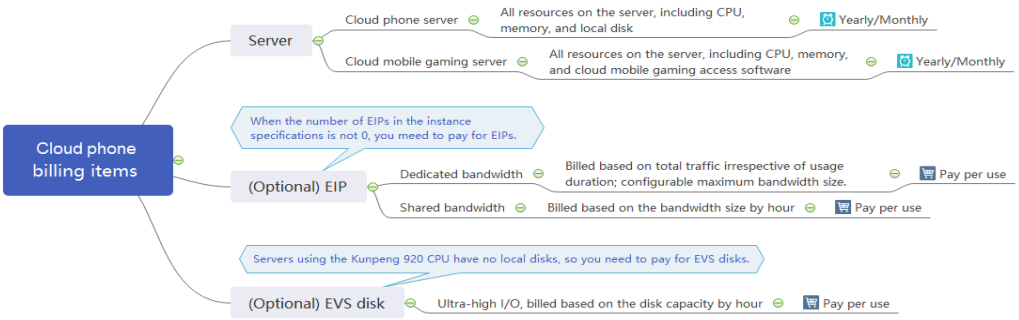


Table 7-1 Billing items

Billing Item	Description	Example	Billing Mode
Server	You obtain cloud phones only after purchasing a server. You pay for all resources on the server. • Server for general-purpose cloud phones: CPU, memory, and local disk • Server for gaming cloud phones: CPU, memory, local disk, and cloud mobile gaming access software	Resource prices may vary by region. The actual prices are subject to those displayed on the management console. For details about how to select a region, see **Region and AZ**.	Yearly/ Monthly
(Optional) EIP	If the number of EIPs is not 0 in the instance specifications, pay for the EIP traffic or bandwidth. The billing standard varies depending on the bandwidth type. • Dedicated bandwidth: billed based on total traffic irrespective of usage duration; configurable maximum bandwidth size • Shared bandwidth: billed based on the bandwidth size by hour For details, see **Price Calculator**.	Take CN-Hong Kong as an example. The billing standard of the shared bandwidth is $ 0.034 USD/Mbit/s. If you purchase a 50 Mbit/s bandwidth, the price is: 0.034 × 50 = 1.7 (USD/hour)	Pay per use

Billing Item	Description	Example	Billing Mode
(Optional) EVS disk	**physical.kg1.4xlarge.cp**, **physical.kg1.4xlarge.cg**, **physical.rx2.32xlarge.4** and **physical.rx3.32xlarge.4** servers do not have local disks. By default, the system purchases one or more ultra-high I/O EVS disks that will be billed based on the disk capacity by hour. For details, see **Price Calculator**.	Take CN-Hong Kong as an example. The billing standard of ultra-high I/O EVS disks is $0.0004 USD/hour/GB. If you purchase a physical.rx2.32xlarge.4 server, the price is: 0.0004 × 400 × 3 = 0.48 (USD/hour) 400 indicates the EVS disk capacity. 3 indicates the number of EVS disks.	Pay per use

Billing Mode

The cloud phone servers are billed in yearly/monthly mode and do not support the pay-per-use mode. If you want to use CPH for a long time, purchase them by year to save more.

Renewal

To renew a cloud phone server, locate it and click **Renew** in the upper left corner of the server list. Complete the renewal on the displayed **Renew** page. For more information about renewal, including auto-renewal, exporting the renewal list, and changing subscriptions, see **Renewal Management**.

The EIPs and EVS disks associated with cloud phones are billed on a pay-per-use basis. Ensure that your account balance is sufficient to prevent the resources from being frozen and unavailable due to arrears.

Stopping Billing

If you want to stop being charged for the EIP or EVS disk associated with your cloud phone server, you must unsubscribe from the server.

Helpful Links

- **How Long Will Resources Be Released After My Server Expires?**
- **Renewing a Server**
- **Unsubscribing from a Server**

8 Permissions Management

If you need to assign different permissions to personnel in your enterprise to access your CPH resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you to securely access your Huawei Cloud resources.

With IAM, you can create IAM users and assign permissions to control their access to specific Huawei Cloud resources. For example, if you want some software developers in your enterprise to view CPH resources but do not want them to restart cloud phones or perform any other high-risk operations, you can create IAM users and grant permission to view CPH resources but not permission to restart cloud phones.

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 **What Is IAM?**

CPH 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.

CPH is a project-level service deployed for specific regions. When you set **Scope** to **Region-specific projects** and select the specified projects (for example, **ap-southeast-1**) in the specified regions (for example, **CN-Hong Kong**), the users only have permissions for CPH in the selected projects. If you set **Scope** to **All resources**, the users have permissions for CPH in all region-specific projects. When accessing CPH, the users need to switch to the authorized region.

You can grant permissions by using roles and policies.

- Roles: A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. Only a limited number of service-level roles are available for authorization. Huawei Cloud services depend on each other. When you grant permissions using roles, you also need

to attach any existing role dependencies. Roles are not ideal for fine-grained authorization and least privilege access.

- 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. For example, you can grant users only permission to manage ECSs of a certain type. A majority of fine-grained policies contain permissions for specific APIs, and permissions are defined using API actions. For the API actions supported by CPH, see **Permissions Policies and Supported Actions**.

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

Table 8-1 System-defined permissions for CPH

Role/Policy Name	Description	Type	Dependencies
CPH Administrator	Administrator permissions for CPH. Users with these permissions can perform all operations on cloud phone servers.	System-defined role	For servers that use custom networks, the **VPC FullAccess** permissions are required. Select dependent roles in the same project.
CPH User	Read-only permissions for CPH. Users with these permissions can only view data about cloud phone servers.	System-defined role	Dependent on the **Tenant Guest** policy.
CPH FullAccess	Users with these permissions can perform all operations defined in the actions supported by CPH.	System-defined policy	If the permissions are not supported by CPH actions, you can use roles to assign permissions.
CPH ReadOnlyAccess	Users with these permissions can only view data about cloud phone servers.	System-defined policy	If the permissions are not supported by CPH actions, you can use roles to assign permissions.

Role/Policy Name	Description	Type	Dependencies
CPH NotSupportEnterpriseAccess	Enterprise project fine-grained actions that are not supported by CPH. CPH users who want to use enterprise projects and use all CPH functions need to obtain the permissions in the **CPH FullAccess** policy (granted **By Enterprise Project**) and the permissions in the **CPH NotSupportEnterpri-seAccess** policy (granted **By IAM Project**).	System-defined policy	If the permissions are not supported by CPH actions, you can use roles to assign permissions.
CPH AgencyDependencyAccess	Fine-grained actions on which CPH depends to create cloud phone servers.	System-defined policy	If the permissions are not supported by CPH actions, you can use roles to assign permissions.

Table 8-2 lists the common operations supported by each CPH system role. Choose proper system roles according to this table.

Table 8-2 Relationship between common operations and system roles

Description	CPH Administrator	CPH User	CPH FullAccess	CPH ReadOnlyAccess	CPH NotSupportEnterpriseAccess
Purchasing a cloud phone server	√	×	√	×	×
Deleting a cloud phone server	√	×	√	×	×
Migrating workloads from a cloud phone server to another server	√	×	√	×	×

Description	CPH Administrator	CPH User	CPH FullAccess	CPH ReadOnlyAccess	CPH NotSupportEnterpriseAccess
Querying cloud phone servers	√	√	√	√	×
Querying details of a cloud phone server	√	√	√	√	×
Querying cloud phone server flavors	√	√	√	√	√
Modifying the name of a cloud phone server	√	×	√	×	×
Changing the flavor of a cloud phone server	√	×	√	×	×
Restarting a cloud phone server	√	×	√	×	×
Pushing a shared storage file	√	×	√	×	×
Querying a shared storage file	√	√	√	√	×
Deleting a shared storage file	√	×	√	×	×
Pushing a shared application	√	×	√	×	×
Deleting a shared application	√	×	√	×	×
Changing a key pair	√	×	√	×	×

Description	CPH Administrator	CPH User	CPH FullAccess	CPH ReadOnlyAccess	CPH NotSupportEnterpriseAccess
Querying encoding servers	√	√	√	√	×
Restarting an encoding server	√	×	√	×	×
Querying the bandwidth used by a cloud phone	√	√	√	√	√
Modifying a shared bandwidth	√	×	√	×	√
Querying cloud phones	√	√	√	√	×
Querying details of a cloud phone	√	√	√	√	×
Querying cloud phone flavors	√	×	√	×	√
Resetting cloud phones	√	×	√	×	×
Restarting a cloud phone	√	×	√	×	×
Stopping a cloud phone	√	×	√	×	×
Editing the name of a cloud phone	√	×	√	×	×
Updating cloud phone attributes	√	×	√	×	×
Exporting data of multiple cloud phones	√	×	√	×	×

Description	CPH Administrator	CPH User	CPH FullAccess	CPH ReadOnlyAccess	CPH NotSupportEnterpriseAccess
Restoring cloud phone data	√	×	√	×	×
Diverting cloud phone traffic	√	×	√	×	×
Expanding the disk capacity of multiple cloud phones	√	×	√	×	×
Obtaining information about the cloud phones to be accessed	√	√	√	√	×
Running ADB shell commands asynchronously	√	×	√	×	×
Running ADB shell commands synchronously	√	×	√	×	×
Querying the execution status of a task	√	√	√	√	√
Querying the execution statuses of all tasks	√	√	√	√	√
Batch adding tags	√	×	√	×	×
Batch deleting tags	√	×	√	×	×

Description	CPH Administrator	CPH User	CPH FullAccess	CPH ReadOnlyAccess	CPH NotSupportEnterpriseAccess
Querying resources by tag	√	√	√	√	×
Querying resource tags	√	√	√	√	×
Querying tags of CPH resources in a project	√	√	√	√	×
Querying cloud phone images	√	√	√	√	√
Deleting a cloud phone image	√	×	√	×	×
Sharing a cloud phone image	√	×	√	×	×
Querying users with whom you shared a cloud phone image	√	√	√	√	×
Stopping sharing of a cloud phone image	√	×	√	×	×
Querying AZs	√	√	√	√	√
Querying subnets	√	√	√	√	√
Querying VPC peering connections	√	√	√	√	√
Deleting a VPC peering connection	√	×	√	×	×

Description	CPH Administrator	CPH User	CPH FullAccess	CPH ReadOnlyAccess	CPH NotSupportEnterpriseAccess
Adding a VPC peering connection	√	×	√	×	×
Exporting details of multiple cloud phones	√	×	√	×	×
Creating an agency	√	×	√	×	√
Checking an agency	√	×	√	×	√

Helpful Links

- What Is IAM?
- Creating a User and Granting CPH Permissions

9 Basic Concepts

This section describes the basic concepts you need to understand before using CPH.

Servers

Servers are physical servers that provide cloud phones. You obtain cloud phones only after purchasing a server. To purchase a server and obtain the corresponding number of cloud phones, you only need to specify the server type, instance specifications, phone image, and required network configuration.

Quantity

Quantity refers to the number of cloud phones that can be virtualized from a server. For example, if **Quantity** is **60**, you can have 60 cloud phones virtualized from a server.

Cloud Phone Images

Cloud phone images are OSs running on cloud phones, for example, Android. Only Android AOSP 7.1.1 is provided. In the future, Huawei EMUI will be provided. However, other OSs from the third-party vendors such as Xiaomi ROM and Apple iOS cannot be provided duo to commercial authorization and architecture inconsistency.

SSH Tunnels

An SSH tunnel is established between an SSH client and an SSH server to forward network data to a specified port for network communication. The SSH tunnel provides automatic encryption and decryption services to ensure data transmission security.

SSH tunnels support three port forwarding modes: local port forwarding, remote port forwarding, and dynamic port forwarding. The directions of local and remote port forwarding are opposite. Local port forwarding is used when accessing a cloud phone. This document focuses on the working principle of local port forwarding.

Assume that local host A1 is the SSH client and remote cloud host B1 is the SSH server. Log in to host B1 from the host A1 through SSH and specify different port

forwarding options (-L, -R, and -D). Then the SSH tunnel between host A1 and host B1 is established and data can be forwarded among different ports.

- Scenarios

  A service is running on the remote cloud server B1 and the port number is 2000. The local host A1 needs to access the service. Assume that the IP address of cloud server B1 is 122.*x.x.x*, and the access address of the service is http://122.*x.x.x*:2000.

- Why is local port forwarding required?

  Generally, only port 22 is enabled on the firewall of the cloud server by default. To access port 2000, modify the firewall. To ensure security, configure the IP addresses that are allowed to access the firewall. However, the public IP address of the cloud server is usually dynamically allocated by the network provider. If the public IP address is changed, the firewall configuration needs to be frequently modified, causing unnecessary troubles.

- What is local port forwarding?

  In local port forwarding, requests sent to the local port are forwarded to the destination port. In this way, the service on the destination port can be accessed. Use the -L option to specify the port to be forwarded. The syntax is as follows:

  ssh -L *Local port: Destination address: Destination port*

  Example:

  ```
  ssh -L 3000:targethost:2000 root@122.x.x.x
  ```
  In this example, after you log in to remote cloud server B1 from local host A1, the requests sent to port 3000 of local host A1 are forwarded to port 2000 of remote cloud server B1.

  As a result, the local host A1 can access services on the remote cloud server B1 by accessing http://122.x.x.x:2000.

- Extended applications

  In the foregoing syntax, the destination address may also be an address of another host. For example, the destination address is a private IP address of the cloud phone, the local host A1 is the local device, and the remote cloud server B1 is the cloud phone server. To access the cloud phone, the command for establishing an SSH tunnel is:

  ssh -L *Local port: Private IP address of the cloud phone*: *Destination port Username@Public IP address of the server*

  In addition, **-N** and **-f** are common options for establishing an SSH tunnel.

  – **-N**: indicates that the SSH server is not connected after the SSH tunnel is established. **-N** and **-f** are usually used together.

  – **-f**: indicates that the SSH tunnel is running in the background.

ADB

ADB is a command line tool to bridge the communications between an Android device and a desktop computer. It is a unique application of the Android OS. You can use ADB commands to perform a variety of operations, such as installing and debugging apps.

NOTE

For more details about the ADB commands, see **What Are Common ADB Commands?** or visit **https://developer.android.com/studio/command-line/adb**.

10 Region and AZ

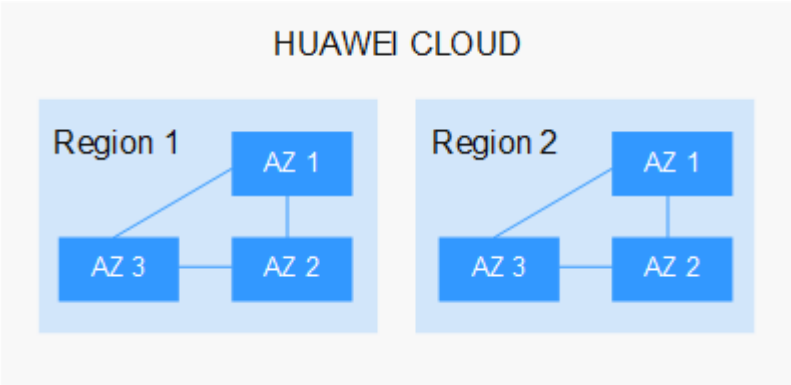
Concept

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 10-1 shows the relationship between regions and AZs.

Figure 10-1 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**.

11 Constraints and Limitations

Notes

- Do not use Huawei Cloud resources for black market or perform activities that violate laws and regulations or Huawei security requirements. If you violate related requirements, your accounts will be restricted or frozen.
- When your Huawei Cloud account is restricted or frozen or your cloud phones are retained, the use of cloud phones will be restricted. You need to handle these issues in advance to avoid service interruptions.
  - If your Huawei Cloud account is restricted due to insufficient balance, you cannot perform operations, such as restarting the cloud phones, replacing images, or pushing files, on cloud phones.
  - If your Huawei Cloud account is in arrears and frozen, you cannot perform operations, such as restarting the cloud phones, replacing images, or pushing files, on cloud phones.
  - If your cloud phones enter the retention period because they are in arrears or have not been renewed upon expiration, the cloud phones will be frozen and cannot be used.
- Cloud phone servers of the physical.kg1.4xlarge, physical.rx2.32xlarge.4, and physical.rx3.32xlarge.4 series use pay-per-use Elastic Volume Service (EVS) disks for storage. Fees are charged by hour in real time. You need to ensure that your account balance is sufficient to prevent resource freezing caused by account arrears.
- You need to keep the access key of the cloud phone secure and exercise caution when selecting the open access port of the cloud phone to ensure security.
- Cloud phone severs of the physical.rx1.xlarge series use local disks to store data. You can periodically back up important data.

Constraints

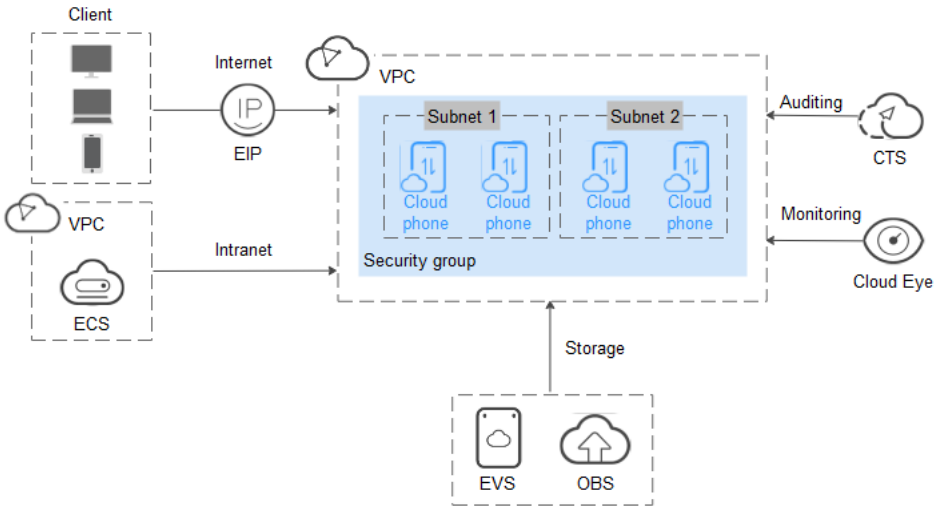
- A cloud phone server runs the native Android OS and has virtual phone functions. It does not have carrier service attributes and does not support functions such as virtual SIM cards, making calls, and sending and receiving SMS messages.
- Cloud phone servers support only the native Android OS. You cannot change the OS or OS type by flashing a ROM or other operations.

- Cloud phone servers do not support secondary virtualization. That is, virtualization software cannot be installed on cloud phone servers.
- Cloud phone servers do not have built-in screenshot and screen recording tools.
- Google Mobile Service (GMS) cannot be installed on cloud phone servers.
- Cloud phone server specifications (for example, **Quantity**) cannot be changed unless you unsubscribe from the current server and purchase one that meets your requirements.
- Cloud phone servers do not support service data migration between different regions or accounts.

12 How CPH Works with Other Services

Figure 12-1 shows relationships between CPH and other services.

Figure 12-1 Relationships between CPH and other services



Related Services

Table 12-1 Related services

Service	Function	Reference
Elastic Cloud Server (ECS)	An ECS can be used as a jump server to connect to a cloud phone through an intranet or as a streaming server in the cloud mobile gaming scenario.	ADB (Intranet)
Elastic IP (EIP)	An EIP enables your cloud phone servers to communicate with external networks.	ADB (Internet)

Service	Function	Reference
Virtual Private Cloud (VPC)	A VPC is used to create a dedicated network environment for your cloud phones.	**Buying a Cloud Phone Server**
Elastic Volume Service (EVS)	EVS provides cloud storage for cloud phones.	• **Servers for General-Purpose Cloud Phones** • **Cloud Mobile Gaming Servers**
Object Storage Service (OBS)	Before installing APKs on cloud phones in batches, you can upload the APKs to the OBS bucket and run the ADB commands to install the APKs.	**Managing Cloud Phones in Batches**
Cloud Eye	After purchasing a cloud phone server, you can view monitoring data of the cloud phone server and related resources (such as cloud phones, disks, and GPU cards) on the Cloud Eye console without installing other plug-ins. You can also obtain visualized monitoring graphs.	• **Supported Metrics** • **Viewing CPH Metrics** • **Creating an Alarm Rule**
Cloud Trace Service (CTS)	Records cloud phone server-related operations for later query, audit, and backtrack.	• **Key Cloud Phone Operations Recorded by CTS** • **Viewing Traces**