Cloud Phone

User Guide

Issue	01
Date	2024-07-31

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 Buying a Cloud Phone Server

Scenarios

Cloud phones are provisioned after you purchase a cloud phone server. The number of cloud phones that can be obtained varies depending on the cloud phone **Quantity**. This section describes how to purchase a cloud phone.

Procedure

1. Log in to the management console.
2. On the **Service List** page, choose **Compute** > **Cloud Phone Host**.
3. In the navigation pane on the left, choose **Servers**. In the upper right corner, click **Buy Server**.
4. Configure required parameters.

Table 1-1 Basic server settings

Parameter	Description	Example Value
Billing Mode	CPH is billed only yearly/ monthly.	Yearly/Monthly
Region	Cloud phone servers in different regions cannot communicate with each other over a private network. For lower latency and quicker access, select the nearest region. After a server is purchased, its region cannot be changed.	CN-Hong Kong

Parameter	Description	Example Value
AZ	An AZ is a part of a region and has its own independent power supplies and networks. AZs can communicate with each other over an internal network and are physically isolated. • If you require high availability, buy servers in different AZs. • If you require low network latency, buy servers in the same AZ.	AZ1
Server Type	Two options are available: **Cloud phone server** and **Cloud mobile gaming server**. For details, see **Servers for General-Purpose Cloud Phones** and **Cloud Mobile Gaming Servers**.	Cloud phone server physical.rx1.xlarge
Instance Specifications	Select the required cloud phone specifications.	rc1.se
Phone Image	Only the Android is supported. **NOTE** To view private images, you must have the **ims:images:list** permissions.	AOSP7.1.1
Quantity	• A maximum of 10 servers can be purchased at a time. • The required duration ranges from 1 month to 3 years.	**Quantity**: **1** Required duration: **6 months**

5. Click **Next: Configure Network** to configure the network for the cloud phone server.

   You are advised to use the custom network described in **Table 1-2**.

Table 1-2 Configuring a custom network

Parameter	Description	Example Value
Network	Select an available VPC and subnet from the drop-down list and specify the method for assigning a private IP address. Ensure that you have the **VPC ReadOnlyAccess** permissions at least. This VPC, including its subnets and security groups will be used to isolate the cloud phone server from the internet. You can also create a VPC. • **IPv6 not required**/**Automatically-assigned IPv6 address**: This parameter is available only for the cloud phone servers with specific flavors and deployed in a VPC with IPv6 enabled in given regions. For details about how to enable IPv6 on a subnet, see **IPv4 and IPv6 Dual-Stack Network**. By default, the system assigns IPv4 addresses. If you select **Automatically-assigned IPv6 address**, the system assigns both an IPv4 address and an IPv6 address. • **Do not configure**/Select the required shared bandwidth: In the same VPC, the cloud phone server can use the IPv6 address to access dual-stack servers. To access the Internet, select a shared bandwidth from the drop-down list and add the IPv6 address to the shared bandwidth. Then, the cloud phone server can access the IPv6 network on the Internet through the IPv6 address. If you do not select a shared bandwidth when creating a cloud phone server, you can manually add your IPv6 address to a shared bandwidth by referring to **(Optional) Step 3: (Optional) Step 3: Buy a Shared Bandwidth and Add the IPv6 Address to It**.	N/A

Parameter	Description	Example Value
	NOTE • If you want to use IPv6 addresses, select **Automatically-assigned IPv6 address** here, and this option cannot be modified after your server is purchased. If you select **IPv6 not required** and want to use IPv6 addresses later, you can only buy a new server. • Due to VPC restrictions, IPv4/IPv6 dual stack is not supported in the CN East-Shanghai 2 region. • IPv6 addresses cannot be added to a dedicated bandwidth. • By default, a maximum of 20 IPv6 addresses can be added to a shared bandwidth. A dual-stack cloud phone server has the same number of IPv6 addresses and virtual IP addresses. If you want to purchase a cloud phone server with multiple virtual IP addresses, such as e0v100, apply for a higher shared bandwidth quota in advance. • RX1 servers do not support IPv6 addresses.	

Parameter	Description	Example Value
Agency	Authorize CPH to create a **cph_admin_trust** agency that can assign **VPC FullAccess** permissions. To authorize CPH to create an agency for you, ensure that you have the **Security Administrator** permissions. For more information, see **Permissions Management**. CPH will use the agency to perform the following operations: • Create an elastic NIC, EIP, and virtual IP address for a cloud phone. • Apply the default security group for the cloud phone server. The default security group defines the port range allowed to access the server. The port range will be mapped to that of each cloud phone. Then the cloud phones can access applications through the mapped ports. **NOTE** By default, if an ECS and a cloud phone are in the same VPC, the ECS cannot access the cloud phone through ports 1 to 9999. If you want to allow such access, add a security group rule with a higher priority by following instructions provided in **What Are the Security Group Authorization Rules for Cloud Phones Using Custom Networks?**	N/A
EIP	• **Auto assign**: Buy a new EIP for the server. • **Using existing**: An existing EIP will be assigned to the server.	Auto assign
EIP Type	• Static BGP offers routing control and protects against route flapping, but cannot choose an optimal path in real time when a network connection fails. • Dynamic BGP enables automatic failovers and chooses the optimal path when a network connection fails.	Dynamic BGP

Parameter	Description	Example Value
Billed By	The following options are available only when a new EIP is purchased: • Traffic: You will be charged based on the total traffic your applications generate. • Shared bandwidth: You will be charged by the bandwidth shared by multiple EIPs.	Shared bandwidth
Bandwidth Size	Value range: 1 Mbit/s to 2,000 Mbit/s	300 Mbit/s
Bandwidth Name	If you set **Bandwidth** to **Shared bandwidth**, select an existing shared bandwidth name from the drop-down list.	bandwidth-001

6. Click **Next: Configure Advanced Settings**.

Table 1-3 Parameters for advanced settings

Parameter	Description	Example Value
Name	Specifies a unique name for the server and its cloud phones. Naming rule: The system automatically adds a hyphen followed by a one-digit incremental number to the end of each server name. For the names of the cloud phones that are virtualized from the server, the system automatically adds a 5-digit number suffix in ascending order. For example, if you purchased a server that can virtualize 60 cloud phones and entered **CPH** for **Name**, the server name is **CPH-1**, and the cloud phone names vary from **CPH-1-00001** to **CPH-1-00060**.	CPH

Parameter	Description	Example Value
Key Pair	A key pair is used for remote login authentication. • If you have created a key pair and stored the private key file (in .pem format) locally, you can select it from the drop-down list. • If no key pair is available, click **Create Key Pair** to create one. Then go back to the **Configure Advanced Settings** page, refresh the drop-down list, and select the created key pair. The private key file is used for identity authentication during remote login. For security purposes, the private key file (in .pem format) can be downloaded only once. Keep it secure. For more information about key pairs, see **(Recommended) Creating a Key Pair on the Management Console**. **NOTE** • Ensure that your account has the **ecs:serverKeypairs:list** permissions to query key pairs. • If you need to create a key pair, ensure that your account has the **ecs:serverKeypairs:create** permissions.	KeyPair-test

Parameter	Description	Example Value
Application Port	Enable this parameter when your cloud phones need to provide services for external systems. • **Application name**: The name can contain letters. However, **ADB** in uppercase, lowercase, or mixed case are not allowed. • **Port number**: Ports from **0** to **65535** are supported. • **Internet access** – If this option is selected, the cloud phone application port can be accessed over the Internet without authentication. The cloud phone port and the server port are accessible from the Internet. – If this option is not selected, cloud phones can be accessed only over a private network. **CAUTION** • Ensure that security control has been performed before you select **Internet access**. • CPH does not perform security check for ports you configured to be accessible from the Internet.	key 10001 Do not select it.

7. Click **Next: Confirm** to check the configuration.
   – If the configuration is correct, click **Buy Now**.
   – To modify the configuration, click **Previous**.
8. Complete the payment as prompted.

   After the payment, it takes the system about 20 to 30 minutes to automatically create cloud phones.

   The cloud phones are available when their statuses change to **Running**.

Follow-up Operations

- To view statuses and IP addresses of servers, go to the **Servers** page. To view names and statuses of cloud phones, go to the **Cloud Phones** page. The number of cloud phones that can be purchased on a server depends on the server specifications you selected. For example, if **Quantity** is set to **60**, 60 cloud phones can be created.

  All cloud phones share the IP address of the server. Each cloud phone has an independent private IP address.
- To access a cloud phone, use ADB. ADB is a common connection method and is supported by cloud phones of all specifications.

- After accessing your cloud phone, you may want to try some advanced functions. For details, see the following links:

  Connecting to a Cloud Phone to Obtain Its Screen

  Modifying the Cloud Phone GPS Location
- You can **modify the shared bandwidth size** (only by calling the API) if it cannot meet your service requirements.

2 Accessing the Cloud Phone

2.1 Access Methods

You can access a cloud phone using 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. This method uses command lines to operate a cloud phone, and is applicable to scenarios like automatic application test.

Comparison Between the Two Access Methods

Table 2-1 Comparison

Access Method	EIP	Screen/CLI Control	Requirement
ADB (Intranet)	Not required	Use command lines to control and operate a cloud phone and use other tools (such as Airtest) to obtain the cloud phone screens.	Use an ECS as a jump server to access the cloud phone.
ADB (Recommended) **ADB (Internet)**	Required one EIP for the server.	Use command lines to control and operate a cloud phone and use other tools (such as Airtest) to obtain the cloud phone screens.	N/A

2.2 ADB (Recommended)

You can use ADB to access your cloud phones on the CPH console. This method is similar to the **ADB (Internet)** method. The access principles are the same.

Prerequisites

The cloud phone must be in the **Running** state.

Procedure

1. Log in to the management console.
2. On the **Service List** page, choose **Compute** > **Cloud Phone Host**.

   The CPH console is displayed.
3. In the navigation pane on the left, choose **Instances**.
4. On the **Instances** page, locate the target cloud phone, and choose **More** > **Access Through ADB** in the **Operation** column.

   The right pane is displayed.
5. Enter the local path for storing the private key file of the server, for example, **C:\Users\Administrator\Downloads\KeyPair-a49c.pem**.
6. Enter the **platform-tools** directory. To obtain the directory,

   download the ADB tool and decompress the tool package to a specified directory, for example, **C:\Users\Administrator\Downloads\platform-tools**.

   NOTE

   If you cannot access the ADB download address on the console, click the following link to download ADB:

   https://dl.google.com/android/repository/platform-tools-latest-windows.zip
7. Enter a local idle port number.

   Run the **netstat -an** command to check whether the port is idle.

   As shown in the following figure, port 6667 is occupied by another program, and port 1234 is idle.

8. After you performed **5**, **6**, **7** in the lower part of the right panel, the command is automatically filled in the blank area. Perform operations as prompted to access the cloud phone.

   For details about the parameters in the command for establishing an SSH tunnel, see **ADB (Internet)**.

NOTE

If you select **Automatically-assigned IPv6 address** when purchasing a cloud phone server, you can use the IPv6 address of the server to establish a tunnel to connect to the cloud phone. The command structure is the same as that for an IPv4 address. The following is an example:

ssh -L 1234:[fd00::aed:96]:5555 05e1aexxx@ xxx:xxx:xxx:xxx -i C:\Users \Administrator\Downloads\KeyPair-a49c.pem -o ServerAliveInterval=30 -Nf

For details about how to troubleshoot SSH tunnel establishment faults, visit the following links:

- **What Can I Do If the SSH Tunnel Fails to Be Established When I Access the Cloud Phone over the Public Network?**
- **What Can I Do If Message "too open" Is Displayed When I Am Establishing the SSH Tunnel?**
- **What Can I Do If Message "Permission denied" Is Displayed When I Am Establishing the SSH Tunnel?**
- **What Can I Do If Message "no match mac found" Is Displayed When I Am Establishing the SSH Tunnel?**
- **How Do I Keep an SSH Session Uninterrupted?**

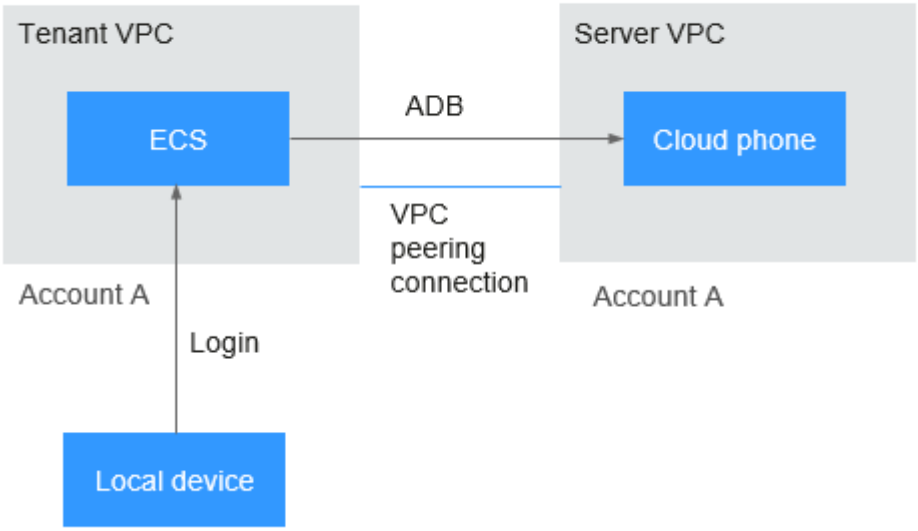
Helpful Links

- **Connecting to a Cloud Phone to Obtain Its Screen**
- **How Do I Install Applications on a Cloud Phone?**

2.3 ADB (Intranet)

When you connect to a cloud phone through a private network, create an ECS in your VPC as the jump server for connecting to the cloud phone. If you do not customize the network when buying a cloud phone server, create a VPC peering connection between your existing VPC and the VPC where the cloud phone server is located, as shown in **Figure 2-1**. The ECS can run either the Windows or Linux. This topic uses the Windows as an example.

Figure 2-1 Using ADB to access a cloud phone over an Intranet



Constraints and Limitations

- You cannot establish a peering connection between the VPC of a tenant who has not purchased a server with the VPC where a purchased server is located. For example, in **Figure 2-1**, the tenant VPC and the VPC where the server resides belong to account A. A VPC peering connection across accounts cannot be created.
- The CIDR block of your VPC cannot overlap with 172.31.0.0/16 and 10.237.0.0/16. Otherwise, the VPC peering connection may be invalid.
- If multiple VPC peering connections are established between your VPC and the VPC where the cloud phone server resides, only one of the peering connections is automatically accepted.

Prerequisites

- The cloud phone must be in the **Running** state.
- The inbound rules configured for your VPC allow traffic from the IP address and port of the cloud phone to be accessed.

  To obtain the IP address and port number of a cloud phone, go to its details page and obtain the server listening address in the **Application Port** area.

  Figure 2-2 Application Port

  Application Port

Application Name	Instance Listening IP Address	Server Listening IP Address
adb	10.237.0.61:5555	172.31.56.147:4673

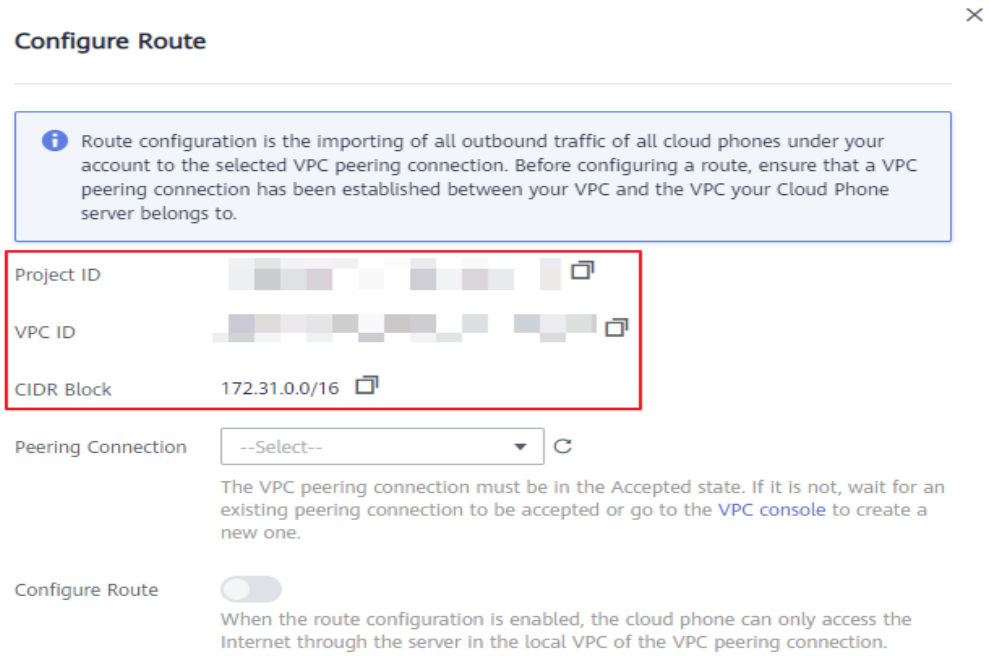
- A Windows ECS is available in your VPC.
- If you want to use an IPv6 address to connect to a dual-stack cloud phone, ensure that your environment, such as your ECS, supports IPv6 addresses.

Step 1: Create a VPC Peering Connection (Only When the Jump Server and the Cloud Phone Are in Different VPCs)

1. Log in to the management console.
2. On the **Service List** page, choose **Compute** > **Cloud Phone Host**.

   The CPH console is displayed.
3. In the navigation pane on the left, choose **Servers**. In the upper part of the server list, click **Configure Route**.
4. In the right pane, record the project ID, VPC ID, and CIDR Block that will be required for creating a VPC peering connection.

   Figure 2-3 Information collection



5. If there is no **Accepted** peering connection available, click **VPC console** to create a VPC peering connection.

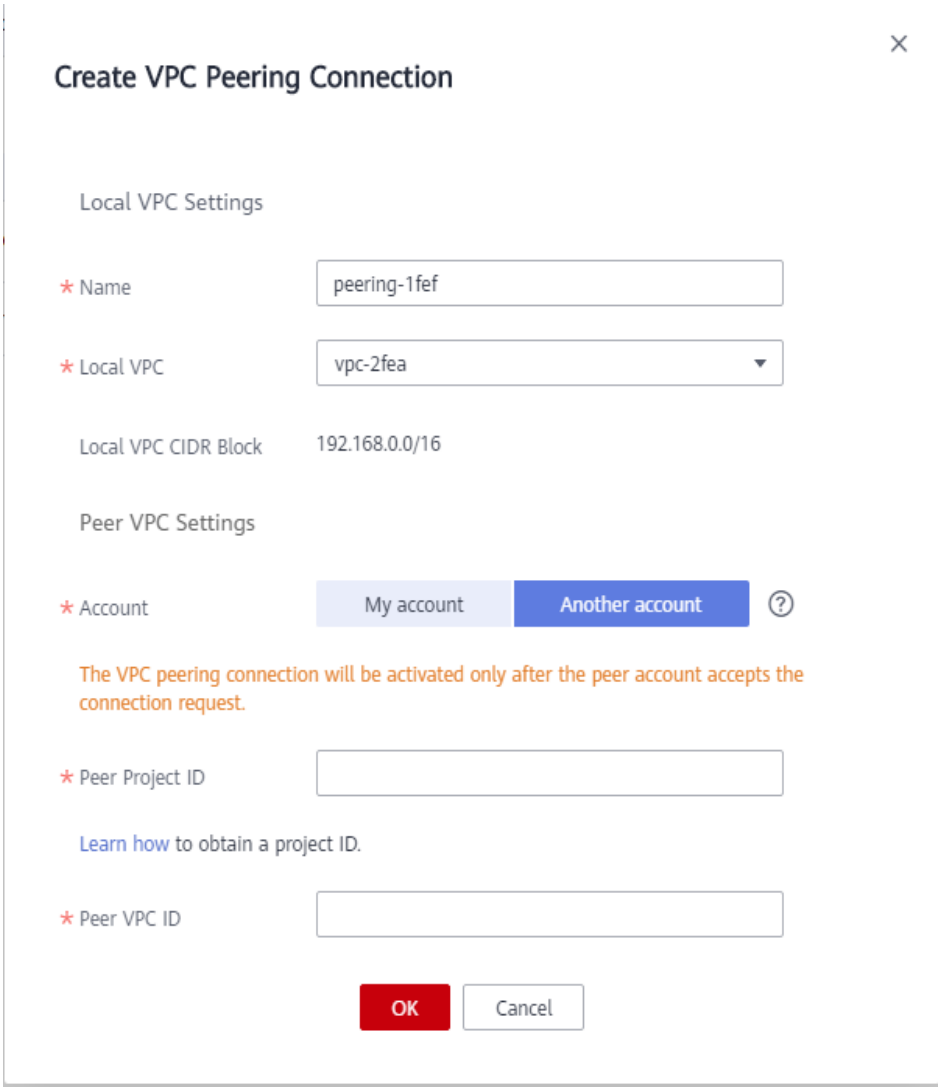
   The **VPC Peering** page is displayed.

   NOTE

   If a VPC peering connection in the **Accepted** state exists, perform the following operations to go to the **VPC Peering** page:

   1. Choose **Service List** > **Network** > **Virtual Private Cloud**.
   2. In the navigation pane on the left, click **VPC Peering**.
6. In the upper right corner, click **Create VPC Peering Connection**.
7. Set parameters as prompted. Set **Account** to **Another account**, **Peer Project ID** to the project ID recorded in **4**, and **Peer VPC ID** to the VPC ID recorded in **4**. Click **OK**.

Figure 2-4 Create VPC Peering Connection



8. Wait for about 5 minutes until the VPC peering connection state changes to **Accepted**.
9. Add routes for the VPC peering connection. For details, see **Step 3: Add Routes for the VPC Peering Connection**. In some regions, you cannot visit the route table module directly from the navigation pane on the left of the network console. In this case, add routes for the VPC peering connection by referring to **Step 3: Add Routes for the VPC Peering Connection**.

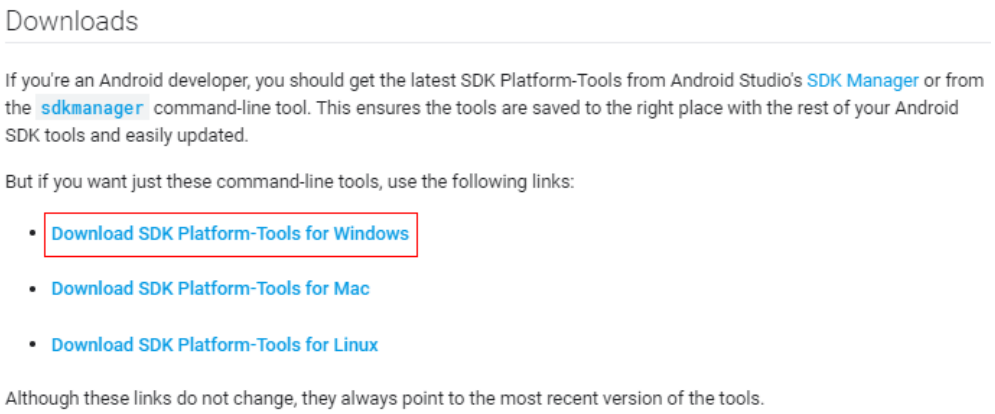
   When adding a route, set **Destination** to the CIDR block recorded in **4**. After the route is added, the two VPCs can communicate with each other.
10. (Optional) If you want to forward all outbound traffic of all of your cloud phones to the created VPC peering connection, perform operations by referring to **Configuring a Route**.

Step 2 Access the Cloud Phone Through ADB

1. Log in to the ECS.
2. Download ADB from the local PC and upload it to the ECS.

Visit **https://developer.android.com/studio/releases/platform-tools**, switch the language to English in the upper right corner, and choose **Download SDK Platform-Tools for Windows**.

Figure 2-5 Downloading ADB



In the displayed dialog box, select the **I have read and agree with the above terms and conditions** check box, and click **DOWNLOAD ANDROID SDK PLATFORM-TOOLS FOR WINDOWS**.

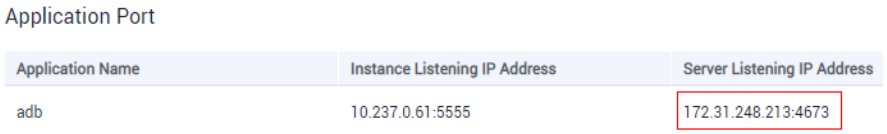
3. Decompress the ADB installation package (for example, **platform-tools_r29.0.5-windows.zip**) to the specified directory (PATH) on the ECS.
4. Go to the **PATH\platform-tools** directory.
5. Run the following ADB command to access the cloud phone:

   adb connect *Listening IP address of the server: Listening port number of the server*

   To obtain the listening IP address and port number of the server, perform the following steps:

   a. On the **Instances** page, click the name of the target cloud phone.
   b. In the **Application Port** area, obtain the listening IP address of the cloud phone server.

   Figure 2-6 Application Port

   Take the information in **Figure 2-6** as an example. Run the following ADB command:

   adb connect 172.31.248.213:4673

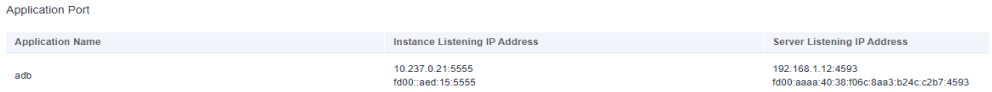
   If you select **Automatically-assigned IPv6 address** when purchasing a cloud phone server, the system will allocate an IPv4 address and an IPv6 address to both the cloud phone and the server, as shown in **Figure 7**. The listening ports of the cloud phone's IPv4 and IPv6 addresses are the same, so are the listening ports of the cloud phone server.

To use the IPv6 address to connect to the cloud phone, run the following ADB command:

adb connect [2409:8c85:80:32:cb7e:97e3:e424:1286]:4615

(Make sure you use square brackets to enclose the IPv6 address.)

Figure 2-7 Application Port



6. Run the **adb devices** command to check whether the current port is connected.

   If information similar to the following is displayed, the connection is successful:

   ```
   List of devices attached
   172.31.248.213:4673  device
   ```

7. Run other ADB commands to operate the cloud phone.

NOTE

For details about how to troubleshoot the ADB connection faults, visit the following links:

- **What Can I Do If Message "unable to connect to :5555" Is Displayed When I Am Using ADB to Access a Cloud Phone?**
- **What Can I Do If the ADB Connection Is Interrupted Suddenly?**

Helpful Links

- **Connecting to a Cloud Phone to Obtain Its Screen**
- **How Do I Install Applications on a Cloud Phone?**

2.4 ADB (Internet)

An EIP is bound to a server, not to the cloud phones virtualized from the server. When you access a cloud phone over the Internet, establish an SSH tunnel first. That is, use the ADB (Internet) method, which includes two steps: establishing an SSH tunnel, and accessing the cloud phone through ADB. For details about the SSH tunnel and ADB, see **Basic Concepts**.

Use a local device (recommended) or a cloud server to access your cloud phone. The local device can run Windows, Linux, Android, or macOS. This topic uses the Windows as an example.

Prerequisites

- The cloud phone must be in the **Running** state.
- If you want to use an IPv6 address to connect to a dual-stack cloud phone, ensure that your environment, such as your ECS, supports IPv6 addresses.

Preparations

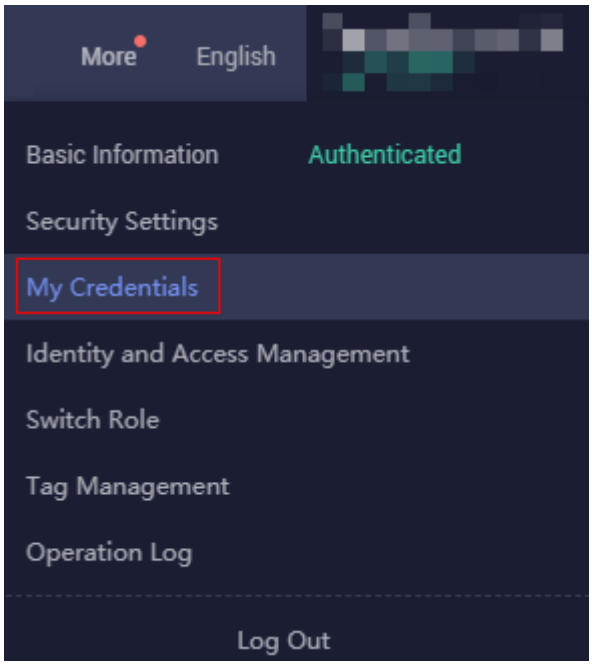
Before establishing an SSH tunnel, ensure that the SSH service has been installed on the local device that will be used to access the cloud phone. (For details, see

How Can I Know Whether the SSH Service Has Been Installed on My Local Device?) You also need to log in to the CPH console and complete the following preparations:

1. Obtain the project ID of the region where the target cloud phone is located.

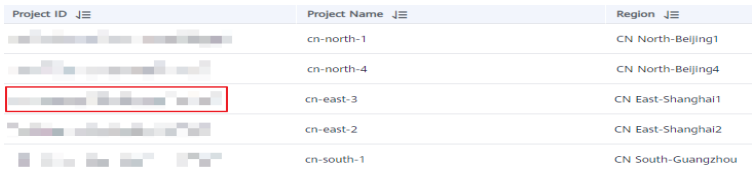
   The operations are as follows:

   a. Locate the username in the upper right corner, hover the mouse over it, and select **My Credentials** from the drop-down list.

   b. Choose **API Credentials**. In the **Projects** area, obtain the project ID of the region where the cloud phone to be accessed is located.

   Example: region **CN East-Shanghai1**

   NOTE

   If the project ID contains more than 32 characters, the first 32 characters are used as the username of the SSH tunnel to be established.

2. Select an idle port on the local device to connect to the cloud phone.

   Run the **netstat -an** command to check whether the port is idle.

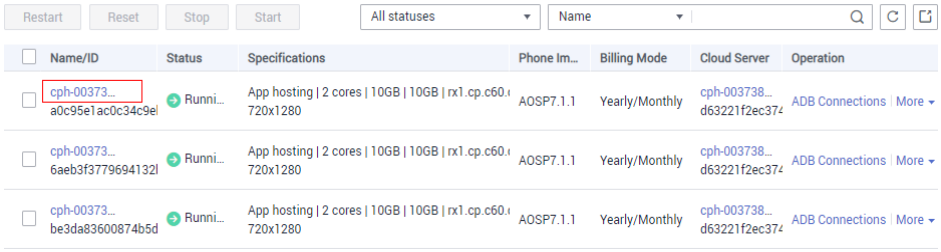
   As shown in the following figure, port 6667 is occupied (displayed as **LISTENING**) by another program, and port 1234 is idle.

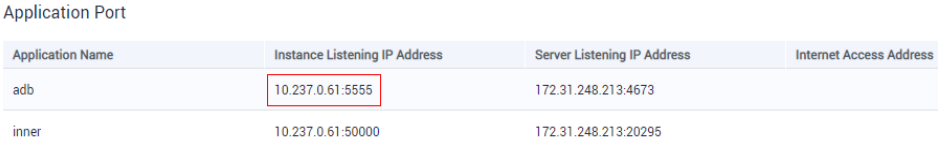
3. Obtain the listening IP address of the cloud phone, that is, the internal IP address and port number of the cloud phone.

   The operations are as follows:

   a. On the CPH console, in the left navigation pane, choose **Instances**, and click the name of the target cloud phone.

   b. In the **Application Port** area, obtain the listening IP address of the cloud phone.

   NOTE

   - If you have customized the application port in **Advanced Settings** when purchasing a server, the port information is displayed. The authentication mode of the SSH tunnel is the same as that of using the default ADB port. You only need to replace the listening IP address of the cloud phone with the listening IP address of the cloud phone on the corresponding port.
   - If you select **Internet access** when customizing the application port, the public access address of the port is displayed. You can access the cloud phone over the Internet and this port. However, stay alert to security risks.
   - If you select **Automatically-assigned IPv6 address** when purchasing a cloud phone server, the **Instance Listening IP Address** column will contain two lines of data, and the IPv6 IP address is in the second line. If you want to connect to the cloud phone through an IPv6 address, use this one.

4. Obtain the public IP address of the server.

   The operations are as follows:

   On the CPH console, choose **Servers** in the left navigation pane, locate the target server, and obtain the value of **IP Address**.

   NOTE

   - If there are multiple servers, identify the server from which the cloud phone was virtualized by name. For example, if the cloud phone name is **cph-test-1-00001**, the corresponding server name is **cph-test-1**.
   - If you select **Automatically-assigned IPv6 address** when purchasing a cloud phone server, you can use the IPv6 address of the server to establish a tunnel to connect to the cloud phone. To view the public IPv6 address, go to the server details page or view the **Server Listening IP Address** column in the **Application Port** area in the previous step.

5. Obtain the local path for storing the private key file corresponding to the server key pair, that is, the local path for storing the private key file when the key pair is created in 6, for example, **C:/Users/Administrator/Downloads/KeyPair-a49c.pem**.

   The path is case insensitive.

   NOTE

   If the private key file corresponding to the server key pair is lost, see **What Can I Do If the Private Key File Is Lost?**

Step 1 Establish an SSH Tunnel

1. Open the CLI on your local device. The following uses Windows 10 as an example:

   Press **Win+R**, enter **cmd** in the **Run** dialog box, and press **Enter**.

2. Run the following command to establish an SSH tunnel:

   ssh -L *Local idle port:Cloud phone listening IP address: SSH tunnel username@Public IP address* **-i** *Private key file path* **-o ServerAliveInterval=30 -Nf**

   The parameters are described as follows:

   - *Local idle port*: indicates any selected local idle port. The port is mapped to the cloud phone application port. For details about how to obtain the local idle port, see 2.
   - *Cloud phone listening IP address*: indicates the private IP address and port number of the cloud phone. For details about how to obtain the private IP address and port number, see 3.
   - *SSH tunnel username*: indicates the project ID of the region where the cloud phone is located. For details about how to obtain the project ID, see 1.
   - *Public IP address*: indicates the public IP address of the cloud phone server. For details about how to obtain the public IP address, see 4.
   - *Private key file path*: indicates the local path for storing the private key file corresponding to the server key pair. For details about how to obtain the local path, see 5.

   Assume that the local idle port is **1234**, the listening IP address of the cloud phone is **10.237.0.61:5555**, the SSH tunnel username is **05e1ae***xxx*, the public IP address is *xxx.xxx.xxx.xxx*, and the private key file path is **C:\Users\Administrator\Downloads\KeyPair-a49c.pem**. Run the following command:

   ssh -L 1234:10.237.0.54:5555 05e1ae*xxx***@***xxx.xxx.xxx.xxx* **-i C:\Users\Administrator\Downloads\KeyPair-a49c.pem -o ServerAliveInterval=30 -Nf**

   This command sets up an SSH tunnel from the local PC to the cloud phone. The tunnel uses local port forwarding and listens to port 1234 of the local PC. When port 1234 of the local PC is accessed, the communication data is forwarded to port 5555 of the cloud phone.

   After the command is executed, the SSH program forwards packets through the tunnel in the background. If no error is reported, or "Authorized users only. All activities may be monitored and reported." is displayed, the SSH tunnel is successfully established.

NOTE

If you select **Automatically-assigned IPv6 address** when purchasing a cloud phone server, you can use the IPv6 address of the server to establish a tunnel to connect to the cloud phone. The command structure is the same as that for an IPv4 address. The following is an example:

ssh -L 1234:[fd00::aed:96]:5555 05e1ae*xxx*@ *xxx:xxx:xxx:xxx* -i C:\Users\Administrator\Downloads\KeyPair-a49c.pem -o ServerAliveInterval=30 -Nf

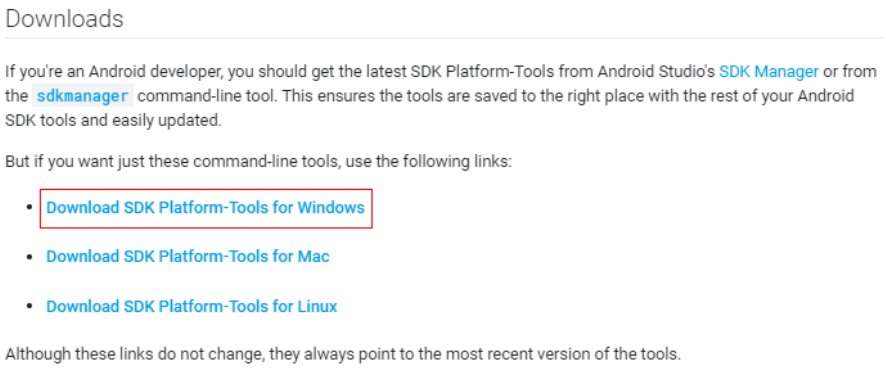
For details about how to troubleshoot SSH tunnel establishment faults, visit the following links:

- **What Can I Do If the SSH Tunnel Fails to Be Established When I Access the Cloud Phone over the Public Network?**
- **What Can I Do If Message "too open" Is Displayed When I Am Establishing the SSH Tunnel?**
- **What Can I Do If Message "Permission denied" Is Displayed When I Am Establishing the SSH Tunnel?**
- **What Can I Do If Message "no match mac found" Is Displayed When I Am Establishing the SSH Tunnel?**
- **How Do I Keep an SSH Session Uninterrupted?**

Step 2 Access the Cloud Phone Through ADB

1. Download ADB.

   Visit **https://developer.android.com/studio/releases/platform-tools**, switch the language to English in the upper right corner, and choose **Download SDK Platform-Tools for Windows**.

   In the displayed dialog box, select the **I have read and agree with the above terms and conditions** check box, and click **DOWNLOAD ANDROID SDK PLATFORM-TOOLS FOR WINDOWS**.

   NOTE

   If you cannot access the preceding website, click the following link to download ADB:

   https://dl.google.com/android/repository/platform-tools-latest-windows.zip

2. Decompress the obtained **platform-tools_r29.0.5-windows.zip** file to a specified directory, for example, **C:\Users\Administrator\Downloads**.

   Version number *29.0.5* in the **platform-tools_r29.0.5-windows.zip** file is only an example.

3. Open the CLI and go to the **C:\Users\Administrator\Downloads\platform-tools** directory.

NOTE

In **Step 1 Establish an SSH Tunnel**, if message "Authorized users only. All activities may be monitored and reported." is displayed, do not close the CLI, and open another CLI to perform this step.

cd C:\Users\Administrator\Downloads\platform-tools

4. Run the following ADB command to access the cloud phone:

   adb connect 127.0.0.1:*Local idle port*

   Local idle port is the idle port used in **2**.

   Example: **adb connect 127.0.0.1:1234**

5. Run the **adb devices** command to check whether the current port is connected.

NOTE

For details about how to troubleshoot the ADB connection faults, visit the following links:

- **What Can I Do If Message "unable to connect to :5555" Is Displayed When I Am Using ADB to Access a Cloud Phone?**
- **What Can I Do If the ADB Connection Is Interrupted Suddenly?**

Helpful Links

- **Connecting to a Cloud Phone to Obtain Its Screen**
- **How Do I Install Applications on a Cloud Phone?**

3 Cloud Phone Management

3.1 Querying Details About a Cloud Phone

This section describes how to query details of a cloud phone on the CPH console.

Procedure

1. Log in to the management console.
2. In the upper left corner, select the region where the target cloud phone is located.
3. On the **Service List** page, choose **Compute** > **Cloud Phone Host**.

   The CPH console is displayed.
4. In the navigation pane on the left, choose **Instances**.
5. Click the name of the target cloud phone to view the following details:
   - **Basic Information**

     Name, **Status**, **Phone ID**, **IMEI**, **Phone Image ID**, and more

     An International Mobile Equipment Identity (IMEI), commonly known as the serial number of a mobile phone, is used to identify an independent mobile communication device such as a mobile phone in the mobile phone network. An IMEI is equivalent to an ID card of a mobile phone. Each cloud phone has a unique IMEI.
   - **Application Port**

     The ports include the default ADB application port and the customized application port during the server purchase. For gaming servers, ports 7000 and 7001 are provided by default for cloud game client access and H5 web page access, respectively.

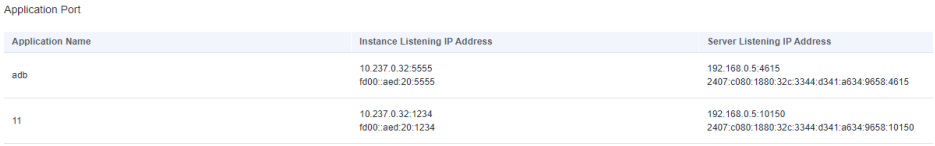
     Figure 3-1 Application port of an IPv4 cloud phone

     Application Port

Application Name	Instance Listening IP Address	Server Listening IP Address	Internet Access Address
adb	10.237.0.61:5555	172.31.248.213:4673	
inner	10.237.0.61:50000	172.31.248.213:20295	

The instance listening IP address and server listening IP address are used to connect to the cloud phone and consist of a private IP address and a port number. Each cloud phone has an independent private IP address.

Figure 3-2 Application port of an IPv4/IPv6 dual-stack cloud phone



If you select **Automatically-assigned IPv6 address** when purchasing a cloud phone server, the system will allocate both an IPv4 and an IPv6 address to both the cloud phone and the server. The listening ports of the cloud phone's IPv4 and IPv6 addresses are the same, so are the listening ports of the cloud phone server.

3.2 Restarting Cloud Phones

This topic describes how to restart a cloud phone or multiple cloud phones on the CPH console.

NOTE

If you use ADB to access a cloud phone, you cannot run the **adb reboot** command to restart the cloud phone because it may cause cloud phone malfunctions. Restart the cloud phone on the CPH console or by calling the CPH API. For details, see **Restarting Cloud Phones**.

Prerequisites

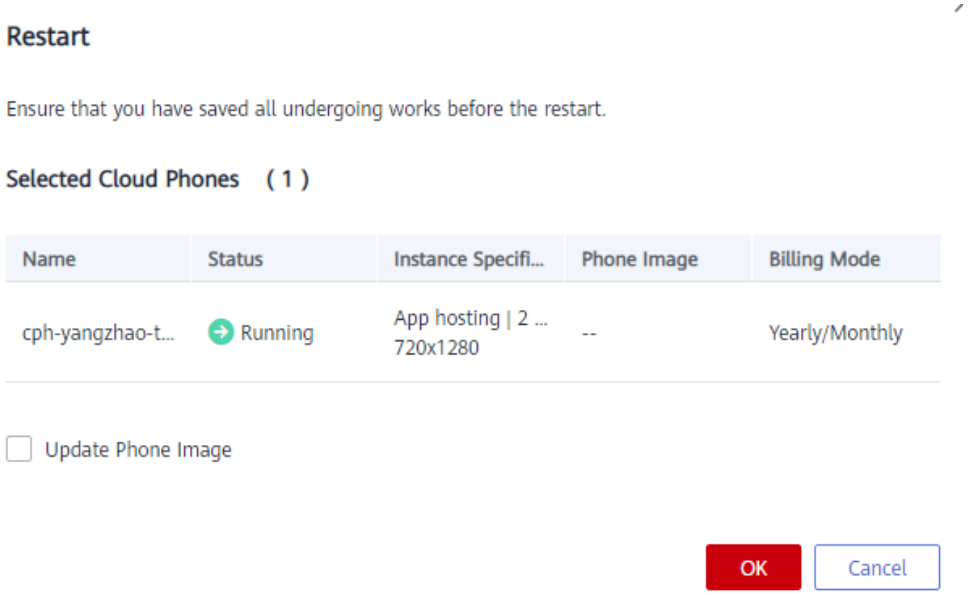
- Before the restart, ensure that all files on the cloud phone have been saved to prevent file loss.
- The cloud phone must be in the **Running** or **Stopped** state. If the cloud phone is in other states, such as **Faulty**, **Stopping**, and **Creating**, it cannot be restarted.

Procedure

1. Log in to the management console.
2. In the upper left corner, select the region where the target cloud phone is located.
3. On the **Service List** page, choose **Compute** > **Cloud Phone Host**.

   The CPH console is displayed.
4. In the navigation pane on the left, choose **Instances**.
5. In the cloud phone list,
   - Select the target cloud phone and click **Restart** in the **Operation** column.
   - Select multiple cloud phones and click **Restart** in the upper left corner of the list.
6. In the right pane, click **OK**.

Figure 3-3 Restart confirmation



If the cloud phone enters the **Restarting** state, the cloud phone is restarted successfully.

NOTE

- You can also select **Update Phone Image** and enter the image ID to update the cloud phone image. If you select multiple cloud phones, you can modify their images in batches.
- You can upgrade an earlier-version AOSP image to a later-version one (for example, from AOSP 7.0 to AOSP 9.0) by restarting a cloud phone. However, in rare scenarios, data of an earlier-version AOSP image may be incompatible with that of a later-version AOSP image. If you do not need to retain user data, reset a cloud phone to upgrade its image to the latest version.

Execution Result

The cloud phone enters the **Running** state.

Associated APIs

Restarting Cloud Phones

3.3 Resetting Cloud Phones

Resetting a cloud phone refers to restoring the cloud phone OS to the initial state, and all data generated on the cloud phone will be deleted. You can perform this operation if the cloud phone system crashes and cannot be recovered.

CAUTION

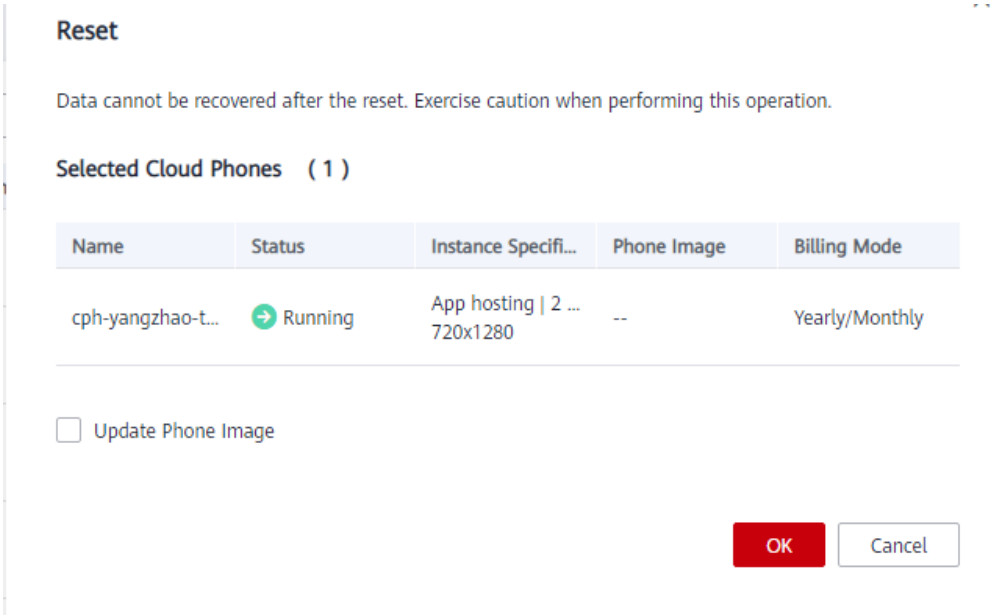
The cloud phone cannot be restored after being reset. Exercise caution when performing this operation.

Procedure

1. Log in to the management console.
2. In the upper left corner, select the region where the target cloud phone is located.
3. On the **Service List** page, choose **Compute** > **Cloud Phone Host**.

   The CPH console is displayed.
4. In the navigation pane on the left, choose **Instances**.
5. In the cloud phone list,
   - Select the target cloud phone and click **Reset** in the **Operation** column.
   - Select multiple cloud phones and click **Reset** in the upper left corner of the list.
6. In the right pane, click **OK**.

Figure 3-4 Reset confirmation



If the cloud phone enters the **Resetting** state, the cloud phone is reset successfully.

NOTE

- You can also select **Update Phone Image** and enter the image ID to update the cloud phone image. If you select multiple cloud phones, you can modify their images in batches.
- If you access a cloud phone through ADB and reset the cloud phone to change its image to an earlier version (for example, from AOSP 9.0 to AOSP 7.0), the cloud phone may be offline. In this case, run the **adb disconnect** *ip:port* command to disconnect the cloud phone, then run the **adb connect** *ip:port* command to reconnect the cloud phone. Then you can view the cloud phone screen.

Execution Result

The cloud phone enters the **Running** state. If the cloud phone is in the **Stopped** state before the reset, it will be automatically started after the reset.

Associated APIs

Resetting Cloud Phones

3.4 Stopping Cloud Phones

This topic describes how to stop a cloud phone or multiple cloud phones on the CPH console.

Prerequisites

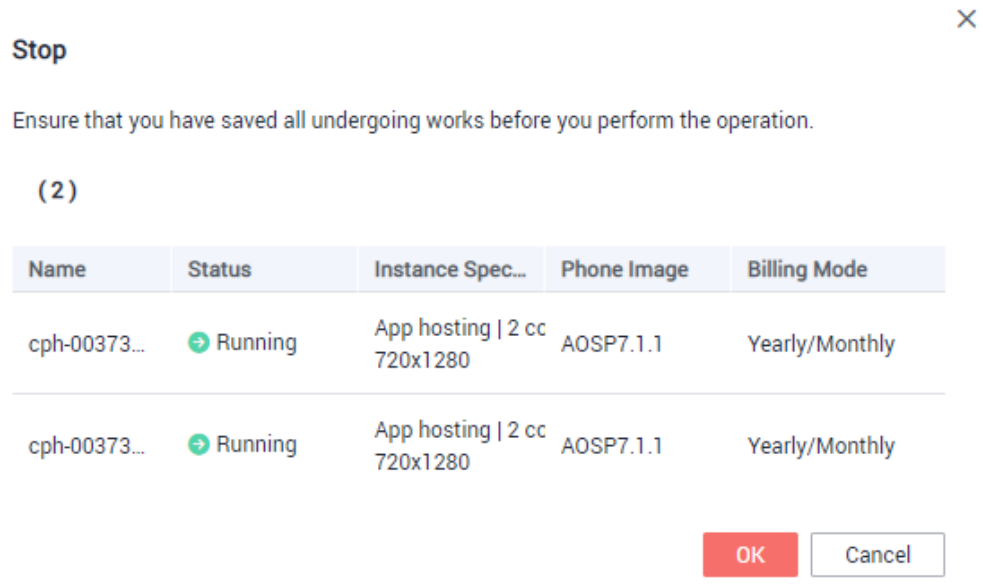
- Before stopping a cloud phone, ensure that all files on it have been saved to prevent file loss.
- The cloud phone must be in the **Running** state. If the cloud phone is in other states, such as **Faulty** and **Creating**, it cannot be stopped.

Procedure

1. Log in to the management console.
2. In the upper left corner, select the region where the target cloud phone is located.
3. On the **Service List** page, choose **Compute** > **Cloud Phone Host**.

   The CPH console is displayed.
4. In the navigation pane on the left, choose **Instances**.
5. In the cloud phone list,
   - Locate the target cloud phone, click **More** in the **Operation** column, and choose **Stop**.
   - Select multiple cloud phones and click **Stop** in the upper left corner of the list.
6. In the right pane, click **OK**.

Figure 3-5 Stop confirmation



If the cloud phone enters the **Stopping** state, the cloud phone is stopped successfully.

Execution Result

The cloud phone enters the **Stopped** state.

Associated APIs

Stopping Cloud Phones

3.5 Editing the Name of a Cloud Phone

This section describes how to edit a cloud phone name on the CPH console.

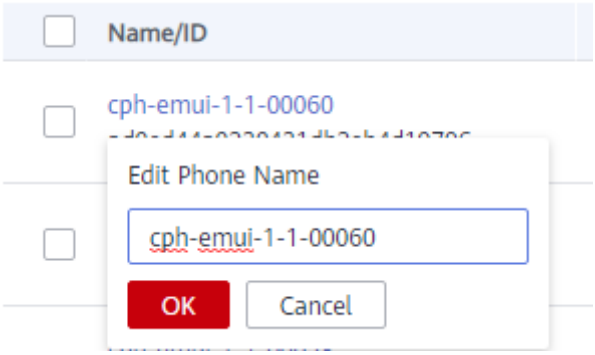
Procedure

1. Log in to the management console.
2. In the upper left corner, select the region where the target cloud phone is located.
3. On the **Service List** page, choose **Compute** > **Cloud Phone Host**.

   The CPH console is displayed.
4. In the navigation pane on the left, choose **Instances**.
5. Locate the target cloud phone, click  next to the name, and enter a new name.

   The name must contain 1 to 60 characters, including only letters, digits, hyphens (-), and underscores (_).

   Figure 3-6 Edit Phone Name

6. Click **OK**.

   The new name will take effect.

Associated APIs

Changing the Cloud Phone Name

3.6 Updating Cloud Phone Attributes

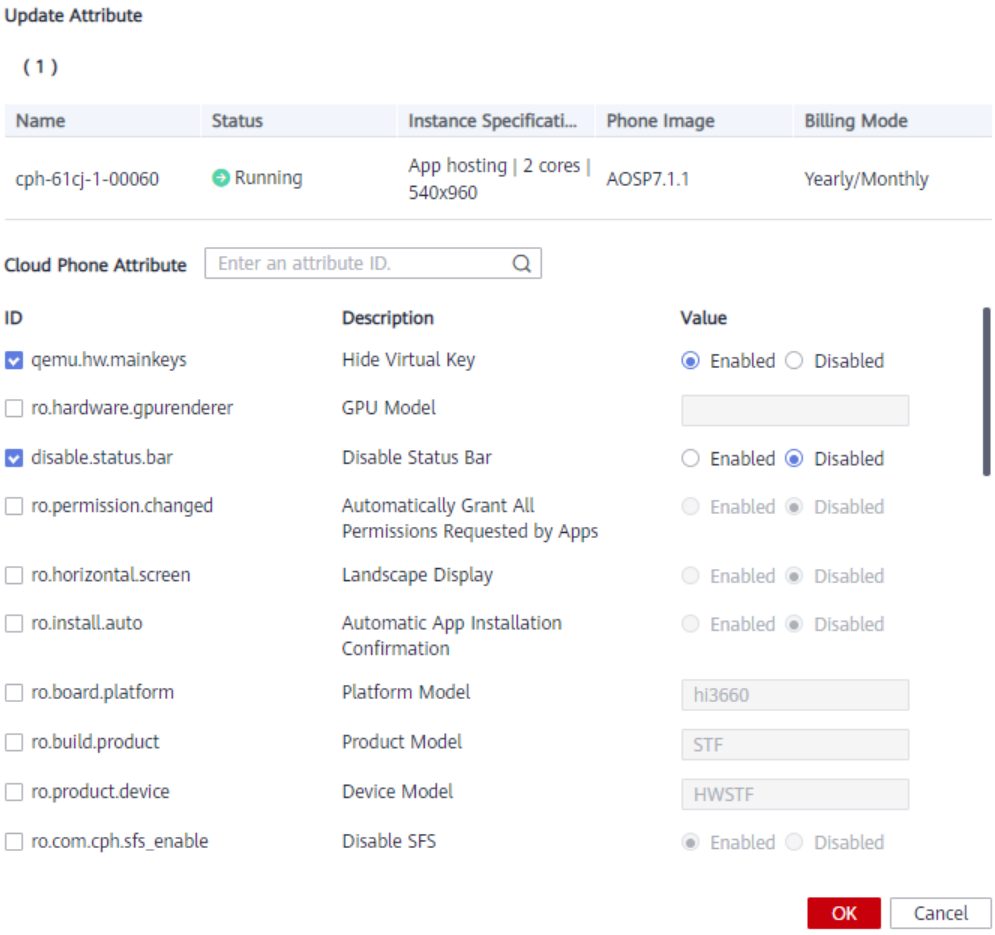
This section describes how to update the cloud phone attributes on the console, such as the product model, device model, whether to hide the virtual key, and whether to display the cloud phone in landscape mode.

Procedure

1. Log in to the management console.
2. In the upper left corner, select the region where the target cloud phone is located.
3. On the **Service List** page, choose **Compute** > **Cloud Phone Host**.

   The CPH console is displayed.
4. In the navigation pane on the left, choose **Instances**.
5. In the cloud phone list, select the target cloud phone, and click **Update Attribute** in the **Operation** column.
6. In the right pane, select the attribute ID, change the attribute value, and click **OK**.

Figure 3-7 Update Attribute



Associated APIs

Updating Cloud Phone Attributes

3.7 Managing Cloud Phones in Batches

By calling the **ADB command API** to push or install the Android package (APK) installation file stored in the Object Storage Service (OBS) bucket to cloud phones in batches, you can efficiently manage cloud phones in batches. This section describes how to install APKs on cloud phones to manage cloud phones in batches.

You can install and update the APK in either of the following ways:

- Run the **install** command through the API. For details, see **Installing the APK**.
- Grant the read permission to the installation package in the OBS bucket to the CPH built-in account, and install and update the APK by file push. For details, see **Pushing Files**.

Constraints and Limitations

CPH has the following restrictions on batch management risk and security:

- The following control commands are supported:

  shell: Enable the remote interactive shell on the cloud phone.

  install: Install the software package on the cloud phone.

  uninstall: Remove the software package from the cloud phone.

  push: Copy a file or folder from the local device to the cloud phone.
- Improper control commands and instructions will cause the cloud phone to malfunction and cannot be recovered.
- To run the **install** or **push** command, strictly follow the instructions in **Procedure**, and build an APK data bucket inclusively used for batch cloud phone management to isolate the data from other data.
- To run the **install** or **push** command, the file must be in .tar format. The files in the compressed package should include all the files required by AOSP.
- On the same cloud phone server, the time consumed by file push is directly proportional to the number of files pushed.

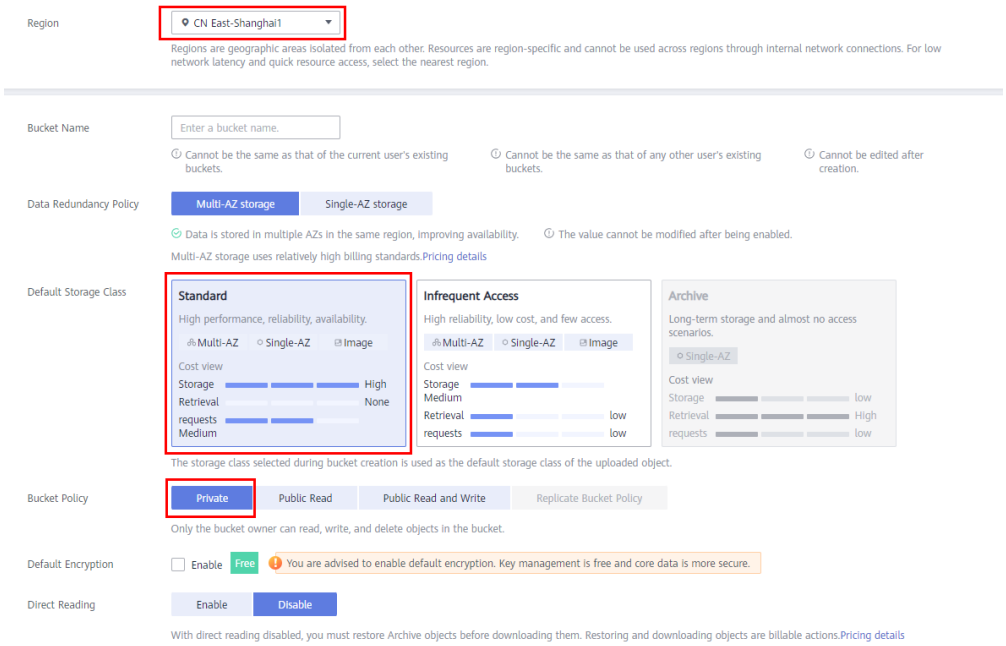
Procedure

The following procedure demonstrates how to create a bucket for storing files and how to set permissions for the bucket. You can install and update APK only by invoking APIs.

1. Log in to the management console.
2. In the **Service List**, choose **Storage** > **Object Storage Service**.

   The **Buckets** page is displayed.
3. In the upper right corner, click **Create Bucket**.

Figure 3-8 Creating a bucket for batch management of cloud phones



- **Region**: Select the region where the cloud phone server is located. The specified region cannot be changed after the bucket is created.
- **Default Storage Class**: Select **Standard**.
- **Bucket Policy**: Select **Private**.

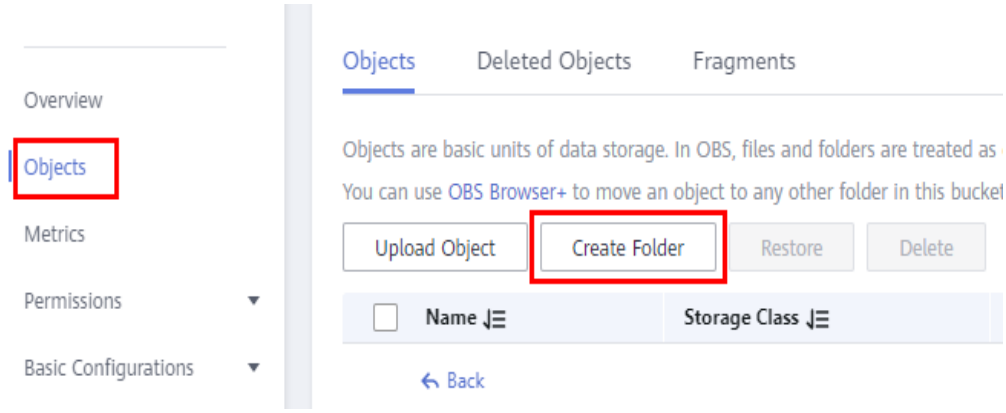
For details about other parameters, see **Creating a Bucket**.

4. Click **Create Now**.

   Wait until the bucket is successfully created.

5. Click the name of the created bucket, choose **Objects** in the navigation pane on the left, and click **Create Folder**.

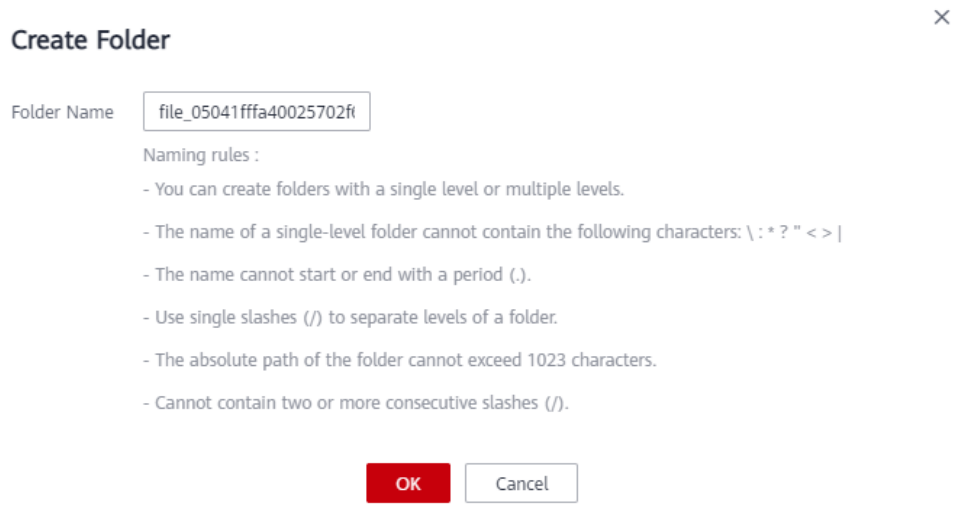
Figure 3-9 Objects



6. Create a folder named **file_{*project_id*}_01** and store files in the **file_{*project_id*}_01** folder.

   {*project_id*} indicates the project ID in the region where the cloud phone server is located. For details about how to obtain the project ID, see **How Do I Obtain the Project ID?**

Figure 3-10 Creating the **file_{*project_id*}_01** folder

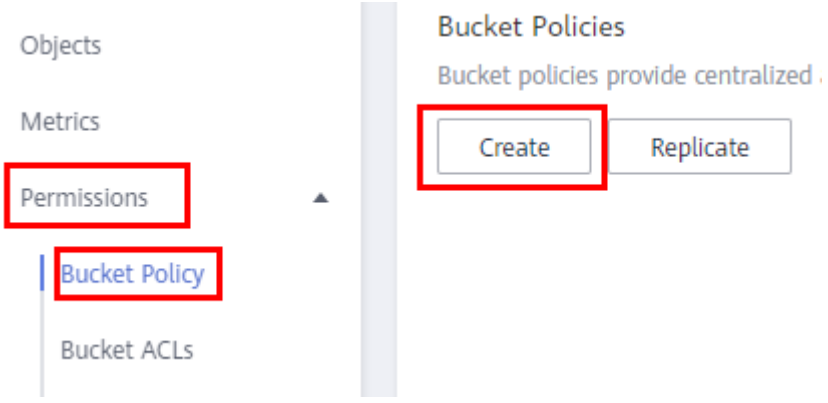


NOTE

- If there are a large number of cloud phones, you can create multiple folders, for example, **file_{*project_id*}_01** and **file_{*project_id*}_02**, to improve the management efficiency.
- Name the folder with a timestamp or function to ease package management, for example, **file_{*project_id*}_01/20190506122012/*xxxx*.tar**.
- If you have hundreds of thousands of cloud phones, develop the application market based on OBS to install and upgrade the APK.

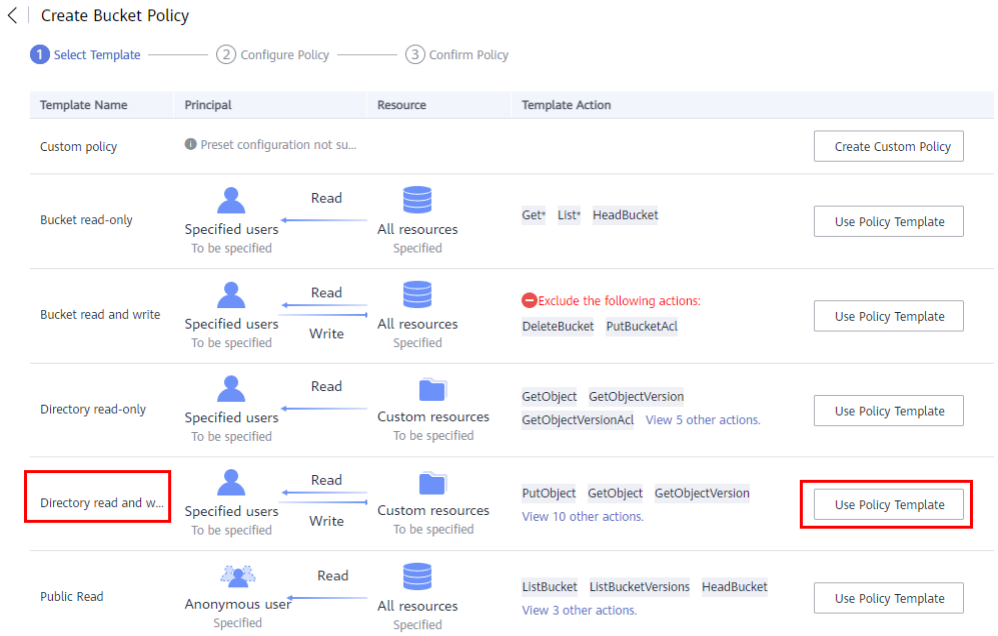
7. In the navigation pane on the left, choose **Permissions** > **Bucket Policy**. On the displayed page, click **Create**.

Figure 3-11 Creating a bucket policy



8. Select **Directory read and write** to grant the read and write permissions of the specified directory in the OBS bucket to the CPH built-in account. Click **Use Policy Template**.

Figure 3-12 Select Template



9. For the **Configure Policy** step, configure the required parameters and click **Next**.
   - **Principal**: Select **Other account**.
   - **Account ID**: Enter the CPH built-in account.

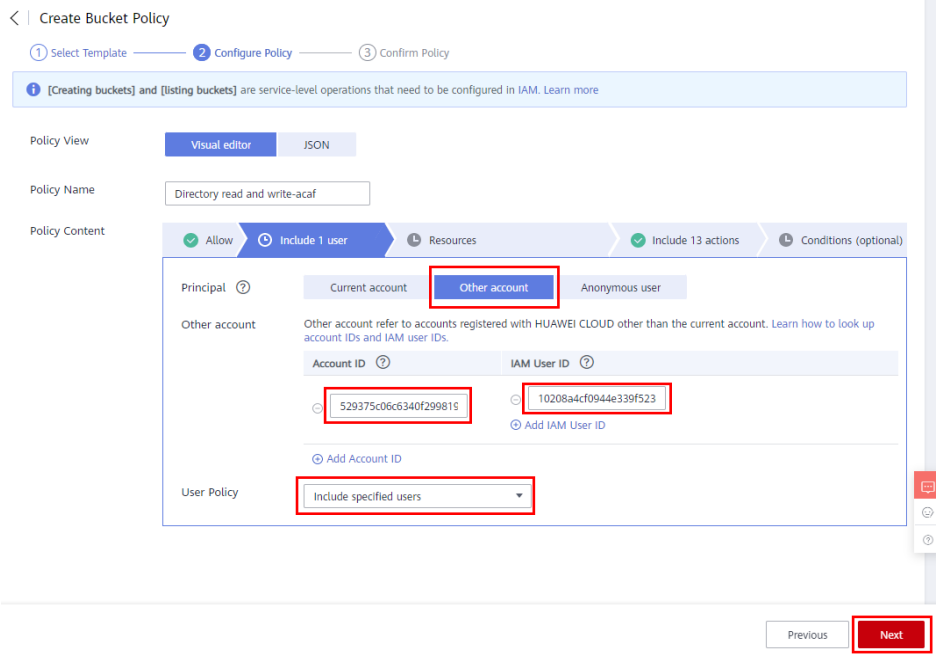
     CAUTION

     The CPH built-in account is mandatory and must contain the following information. You cannot enter the ID of your own account.

     Account ID: **529375c06c6340f299819082b3051225**

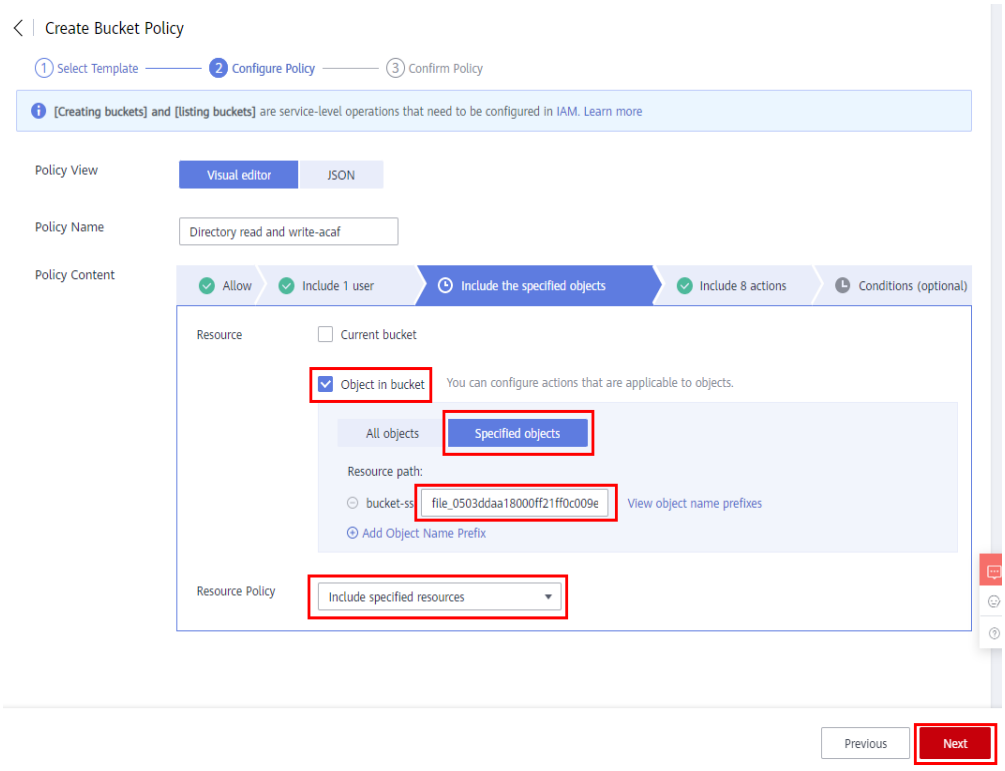
     IAM User ID: **10208a4cf0944e339f523d9943ba02d3**
   - **User Policy**: Select **Include specified users**.

Figure 3-13 Configure Policy



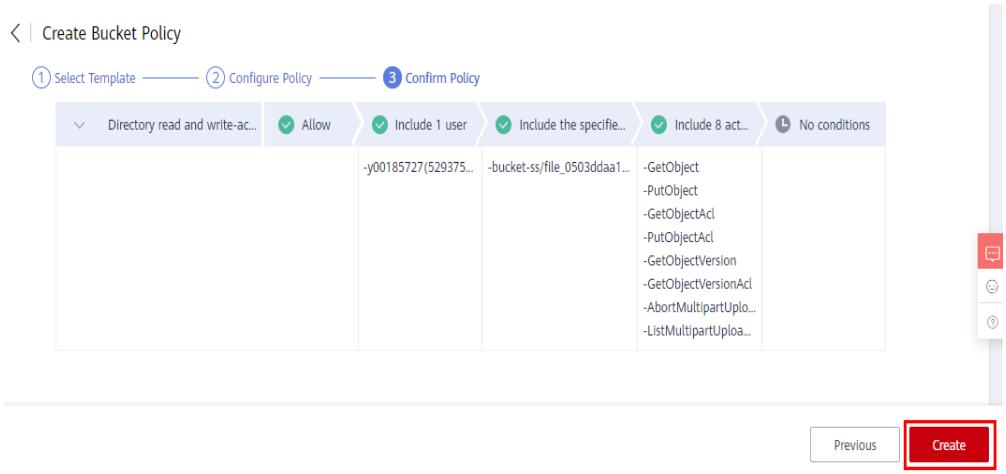
10. For resource, select **Specified object** in the current bucket and enter the resource name **file_{*project_id*}_***, for example, **file_0503ddaa18000ff21ff0c009e65d5482_***. Select **Include specified resources** for **Resource Strategy** and click **Next**.

Figure 3-14 Specified objects



11. Confirm the policy and click **Create**.

Figure 3-15 Confirm Policy



12. Click **Objects**. Place the .tar package to be installed in the **file_{*project_id*}_01** folder. Call the ADB command API to test a cloud phone and check whether the authorization is successful.

    The following ADB command APIs are supported:

    - **Pushing Files**
    - **Installing the APK**
    - **Uninstalling the APK**
    - **Running the Asynchronous ADB shell Commands**

4 Cloud Phone Server Management

4.1 Editing a Server Name

This topic describes how to edit the server name on the CPH console.

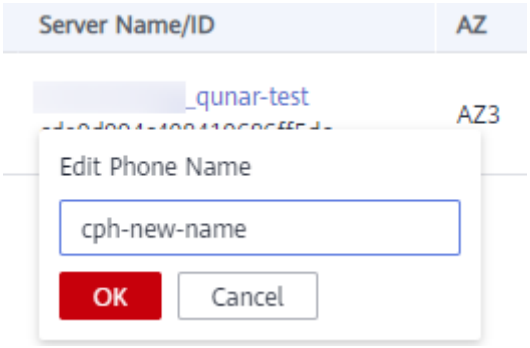
Procedure

1. Log in to the management console.
2. In the upper left corner, select the region where the cloud phone server is deployed.
3. On the **Service List** page, choose **Compute** > **Cloud Phone Host**.

   The CPH console is displayed.
4. In the navigation pane on the left, choose **Servers**.
5. Locate the target server, click  next to the name, and enter a new name.

   The name must contain 1 to 60 characters, including only letters, digits, hyphens (-), and underscores (_).

   Figure 4-1 Edit Server Name

6. Click **OK**.

   The new name will take effect.

4.2 Restarting Servers

This topic describes how to restart a server or multiple servers on the CPH console. When restarting a server, you can update cloud phone images in batches.

Prerequisites

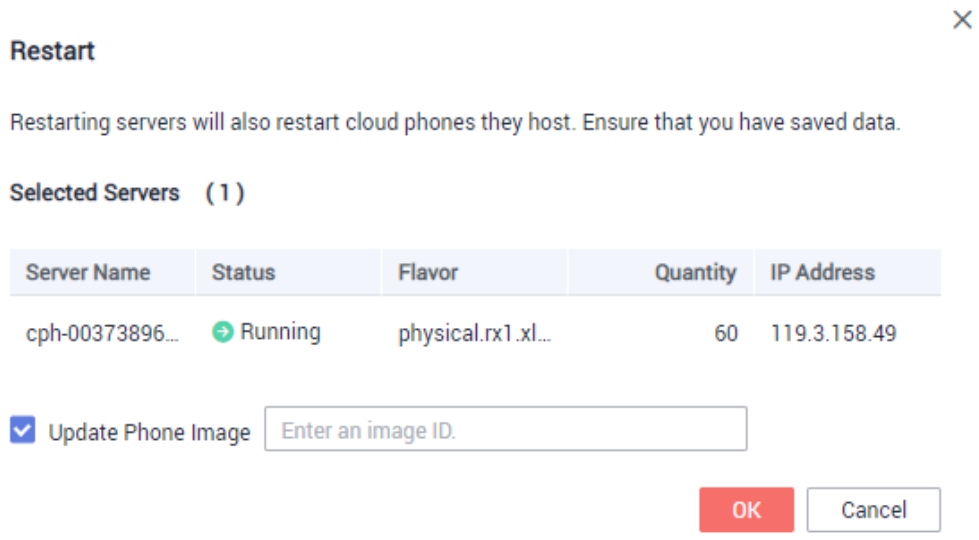
Restarting the server will disconnect the cloud phone. Save data before the restart.

Procedure

1. Log in to the management console.
2. In the upper left corner, select the region where the cloud phone server is deployed.
3. On the **Service List** page, choose **Compute** > **Cloud Phone Host**.

   The CPH console is displayed.
4. In the navigation pane on the left, choose **Servers**.
5. In the server list,
   - Locate the target server, click **More** in the **Operation** column, and choose **Restart**.
   - Select multiple servers and click **Restart** in the upper left corner of the list.
6. In the right pane, click **OK**.

Figure 4-2 Restart confirmation



You can also select **Update Phone Image** and enter the image ID to update cloud phone images in batches.

After the server is restarted, the cloud phone may be abnormal for a short period of time. Wait for a moment. The cloud phone will automatically recover.

Associated APIs

Restarting Cloud Phone Servers In Batches

4.3 Unsubscribing from a Server

Servers are billed yearly/monthly. If you do not want to use a server within the billing period, perform the operations described in this topic to unsubscribe from it.

Notes

- Before unsubscribing from a server, ensure that data on the server has been backed up or migrated. After the unsubscription, the server data will be completely deleted and cannot be recovered. Exercise caution when performing this operation.
- Unsubscribing from yearly/monthly resources refers to unsubscribing from the renewed (if renewed) resources and the resources that are being used. After unsubscription, the resources cannot be used.
- In an unsubscription from a renewal period that has not taken effect, no handling fees are charged. In other cases, a handling fee is billed.

For details about other precautions for resource unsubscription, see **Unsubscription Rules for Reserved Instances**.

Procedure

The following describes how to unsubscribe from a server. If the server has been renewed, you can unsubscribe from the renewal period separately. For details, see **Unsubscribing from a Renewal Period**.

1. Log in to the management console.
2. In the upper left corner, select the region where the cloud phone server is deployed.
3. On the **Service List** page, choose **Compute** > **Cloud Phone Host**.

   The CPH console is displayed.
4. In the navigation pane on the left, choose **Servers**.
5. In the server list, select one or more servers and click **Unsubscribe** in the upper left corner of the list.
6. In the right pane, click **OK**.
7. Confirm the unsubscription information, select the unsubscription reason, and click **Confirm**.

   NOTE

   The page contains a message indicating whether the unsubscription is unconditional within 5 days and the refund account information. Pay attention to the message.

4.4 Renewing a Server

Servers are billed yearly/monthly. If you want to continue using a server before expiration, follow the instructions in this topic to renew it.

Procedure

1. Log in to the management console.
2. In the upper left corner, select the region where the cloud phone server is deployed.
3. On the **Service List** page, choose **Compute** > **Cloud Phone Host**.

   The CPH console is displayed.
4. In the navigation pane on the left, choose **Servers**.
5. In the server list, select one or more servers to be renewed and click **Renew** in the upper left corner of the list.
6. In the right pane, click **OK**.
7. Select the renewal duration, click **Pay**, and pay for the order as prompted.

4.5 Changing an EIP

You can change the EIP bound to a cloud phone server on the **management console** or by **calling APIs**.

NOTE

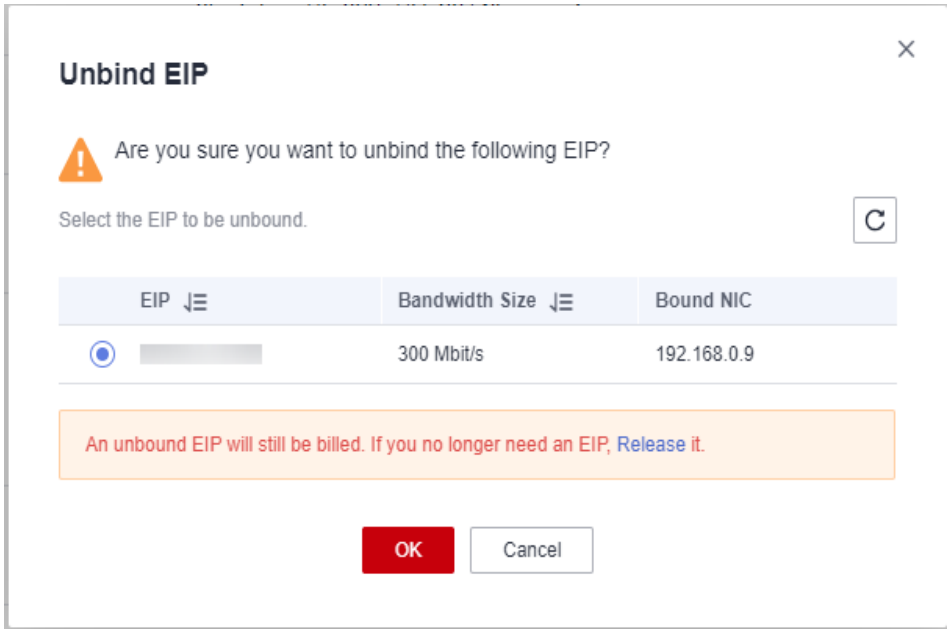
Only EIPs bound to cloud phone servers that use custom networks can be changed. You can go to the details page of a cloud phone server to view its network type.

Changing an EIP on the Console

1. Unbind an EIP.
   a. Log in to the management console.
   b. In the upper left corner, select the region where the cloud phone server is deployed.
   c. On the **Service List** page, choose **Compute** > **Cloud Phone Host**.

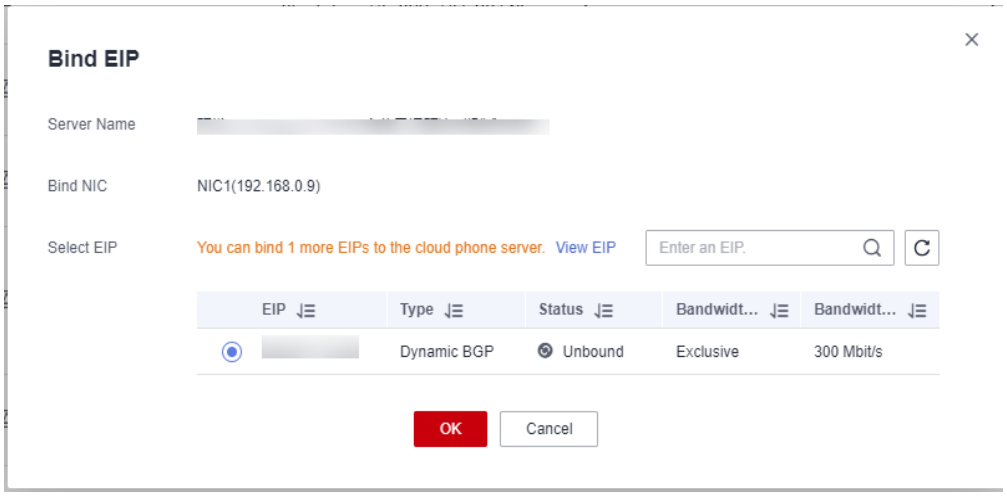
      The CPH console is displayed.
   d. In the navigation pane on the left, choose **Servers**.
   e. In the server list, select the server that needs to change its EIPs, and choose **More** > **Unbind EIP** in the **Operation** column.
   f. In the displayed **Unbind EIP** dialog box, select the EIP to be unbound and click **OK**.

Figure 4-3 Unbind EIP



2. Bind an EIP.
   a. In the server list, select the server to which you want to bind an EIP, and choose **More** > **Bind EIP** in the **Operation** column.
   b. In the displayed **Bind EIP** dialog box, select an EIP, and click **OK**.

Figure 4-4 Bind EIP



Changing an EIP by Calling APIs

1. Unbind an EIP.
   a. Query the EIP address (for example, 122.9.102.*xxx*) of the server on the management console or by calling the **Querying Details About a Cloud Phone Server** API.
   b. Query the EIP ID by IP address on the EIP management console or by calling the **Querying All EIPs** API.

c. Call the **Unbinding an EIP** API.

The following shows an example of an API call:

```
curl -i -k -X POST https://{Endpoint}/v3/{project_id}/eip/publicips/{eip_id}/disassociate-instance -H "Content-Type: application/json" -H "X-Auth-Token: ${token}"
```

2. Bind an EIP.

Strictly speaking, an EIP is bound to a server port. You can bind an EIP to a cloud phone server that has idle ports.

a. Obtain the ID of the EIP to be bound by following the steps **1**. The EIP must be in the unbound state.

b. Call the **Querying Ports** API to query all ports of the server by using **server_id**.

The following shows an example of an API call:

```
curl -i -k -X GET https://{Endpoint}/v1/{project_id}/ports?instance_id={cph_server_id} -H "Content-Type: application/json" -H "X-Auth-Token: ${token}"
```

c. Call the **Querying EIPs** API to query EIPs by using **port_id**. You can specify one or more port IDs at a time. If there is a port that has no EIP bound, you can bind an EIP to the port.

The following shows an example of an API call:

```
curl -i -k -X GET https://{Endpoint}/v1/{project_id}/publicips?port_id={port_id1}\&port_id={port_id2}\&port_id={port_id3} -H "Content-Type: application/json" -H "X-Auth-Token: ${token}"
```

d. If a port has no EIP bound, call the **Binding an EIP** API to bind an EIP to this port.

The following shows an example of an API call:

```
curl -i -k -X POST https://{Endpoint}/v3/{project_id}/eip/publicips/{eip_id}/associate-instance -H "Content-Type: application/json" -H "X-Auth-Token: ${token}" -d '{"publicip": {"associate_instance_id":"{port_id}","associate_instance_type":"PORT"}}'
```


5 Using AOSP

5.1 Overview

You can use the cloud phone AOSP to configure your own init.rc, hide the virtual keys on the cloud phone, set GPS location information, and disable screenshot protection. If you use AOSP, ensure that you are familiar with CPH concepts. For details, see **Service Overview**.

The functions mentioned in the later sections are applicable only to cloud phones in the container solution.

5.2 Automatic Application Authorization

Function

During the application installation, required permissions are automatically assigned to the app.

How to Use

Call the cloud phone API to **update cloud phone attributes** and set **ro.permission.changed** to **1**.

Constraints

- **0** indicates that during the application installation, required permissions are not automatically assigned to the application. **1** indicates that during the application installation, required permissions are automatically assigned to the application.
- The setting takes effect immediately.

5.3 Loading Pictures

Function

This function can be used in code scanning scenarios. For example, inject a QR code to the camera of a cloud phone.

How to Use

1. Obtain the images released on and after October 9, 2020 from **AOSP7 Cloud Phone Image Change History**.
2. Replace the image of the cloud phone with the obtained image ID. Restart the cloud phone and replace the image by clicking **Restart** on the CPH console or calling the **Restarting Cloud Phones** API.
3. Upload the pictures to the **/data/local/tmp/** directory of the cloud phone. Example: **/data/local/tmp/pic.jpeg**
4. Set cloud phone attribute **com.cph.cam_local_pic_path** to **/data/local/tmp/pic.jpeg** (by running the **adb shell** command or call the **Updating Cloud Phone Attributes** API).

   The setting takes effect immediately.
5. Open an application that invokes the camera to view the uploaded picture.

Constraints

- The cloud phone image must be an image released on October 9, 2020 or later. Obtain the image ID from **AOSP7 Cloud Phone Image Change History**.
- The width and height of the picture must be 480*640. If the resolution is not 480 x 640, the picture may be zoomed in or out.
- Only pictures in JPEG and PNG formats are supported.
- The pictures must be stored in the **/data/local/tmp/** directory.
- The picture permission must be at least 644 (rw-r--r--).

5.4 Rooting

Function

By default, applications installed on cloud phones do not have root permissions. CPH lets you centrally grant root permissions to all applications or manage root permissions for each application separately.

How to Use

Grant root permissions to all applications.

If you want all applications on a cloud phone to have root permissions, call the **Restarting Cloud Phones** API and set **ro.com.cph.non_root** to **0**.

Separately manage root permissions for each application.

If you do not want all applications on a cloud phone to have root permissions by default, call the **Restarting Cloud Phones** API and set **ro.com.cph.non_root** to **1**.

Then, you can run commands to manage root permissions for each application separately.

Granting root permissions to a specified application:

```
adb shell cmd activity add-root-permission <PACKAGE>
```

Canceling root permissions for a specified application:

```
adb shell cmd activity remove-root-permission <PACKAGE>
```

Clearing root permissions from all applications with root permissions:

```
adb shell cmd activity clear-root-permission
```

Querying applications with root permissions:

```
adb shell cmd activity show-root-permission
```

Constraints

<*PACKAGE*> indicates the package name of an application. You need to restart the applications for the setting to take effect.

5.5 Startup Script

Function

You can customize the startup script.

How to Use

Push your own script file to the **/data/local/tmp/extend_custom.sh** path.

Constraints

- The script file path must be **/data/local/tmp/extend_custom.sh**.
- The owner group of the file must be **root:root** and the file permission must be 750 (rwxr-x---). If the permission is incorrect, the script cannot be executed.
- The setting takes effect upon restart.

5.6 Automatic Installation of Applications

Function

Install the App. When the **Installer** page is displayed, the application is automatically installed and runs.

How to Use

Call the **Updating Cloud Phone Attributes** API and set **ro.install.auto** to **1**.

Constraints

- **0**: Automatic installation is not performed. **1**: Automatic installation is performed.
- The setting takes effect immediately.

5.7 Hiding Virtual Keys

Function

Cloud phone virtual keys can be hidden.

How to Use

Call the **Updating Cloud Phone Attributes** API and set **com.cph.mainkeys** to **1**.

Constraints

- **0**: Virtual keys are displayed. **1**: Virtual keys are hidden.
- The setting takes effect upon restart.

5.8 Hiding the Status Bar

Function

The cloud phone status bar can be hidden.

How to Use

Call the **Updating Cloud Phone Attributes** API and set **disable.status.bar** to **1**.

Constraints

- **0**: The status bar is displayed. **1**: The status bar is hidden.
- The setting takes effect upon restart.

5.9 Disabling the Notification System

Disabling Notifications from All Applications

Function

The notification system (including the message notification and toast displayed on the top of the screen) will be disabled. The notifications of all applications will be disabled.

How to Use

Call the **Updating Cloud Phone Attributes** API and set **ro.com.cph.notification_disable** to **1**. As a result, the notification system will be disabled. To enable Toast only, set **ro.com.cph.toast_enable** to **1**.

Constraints

- For attribute **ro.com.cph.notification_disable**, value **0** indicates that the notification is allowed, and value **1** indicates that the notification is not allowed.
- For attribute **ro.com.cph.toast_enable**, value **0** indicates that the toast function is disabled, and value **1** indicates that the toast function is enabled.
- The setting takes effect immediately.

Disabling Notifications from Specified Applications

Function

Notification blacklist can be applied. Applications in the blacklist will be forbidden to send notifications.

How to Use

Push the configuration file to the **/data/local/config/NotificationAPP** path.

Constraints

- The configuration format is as follows: ${package_name}

  Examples:

  com.aaa.bbb

  com.aaa.ccc

  com.aaa.ddd
- Set the file permissions to 644.
- The configuration file uses the Unix line feed (\n).
- The setting takes effect immediately.

5.10 Disabling Screenshot Protection

Function

Screenshots are not allowed for some applications in scenarios that have security requirements. If the application that you connect to the cloud phone displays images by transmitting real-time screenshots, a black screen may be displayed on this app. In this case, disable the screenshot protection and restart the cloud phone to view the actual image. By setting **com.cph.disable_fb_permission** to **1**, you can take screenshots.

How to Use

Call the **Restarting Cloud Phones** API and set **com.cph.disable_fb_permission** to **1**.

Constraints

- **0**: Screenshot is forbidden. **1**: Screenshot is allowed.
- The setting takes effect upon restart.

5.11 Simulating Location Information

Function

The simulated positioning information of CPH includes GPS data, base station information, and Wi-Fi Basic Service Set Identifier (BSSID). CPH also provides the geocoding and reverse geocoding.

How to Use

- Injection of GPS data and base station information

Use the adb shell of the cloud phone, and run the **echo "(***parameters***" > /data/gps/fifo** command. Parameters are separated by colons.

Example:

```
echo "longitude=113.370592:latitude=23.123642:cell_type=GSM:mcc=460:mnc=2:lac=37107:cid=263496967"
> /data/gps/fifo
```

- Continuous GPS data injection (Non-blocking injection is recommended.)

Use self-developed or third-party SDK application code to continuously inject GPS data in **O_NONBLOCK** (non-blocking) mode.

Example:

```
#define GPSFifoName "/data/gps/fifo"
if((fifo_fd = open(GPSFifoName, O_WRONLY | O_NONBLOCK)) < 0) {
ALOGE("open fifo "%s" (write) fail, error = %s\n", GPSFifoName, strerror(errno));
return;
}
//Note: Use colons (:) to separate cmd parameters.
char* cmd = "longitude=113.370592:latitude=23.123642:cell_type=GSM:mcc=460:mnc=2:lac=
37107:cid=263496967";
len = strlen(cmd);
if(write(fifo_fd, cmd, len) != len) {
ALOGE("%s: write "%s" to "%s" fail: %s", FUNCTION, cmd, GPSFifoName, strerror(errno));
}
```

- Wi-Fi BSSID simulation

Set **com.cph.wifi.bssid attribute** to simulate which Wi-Fi a cloud phone is connected to.

Example:

```
setprop com.cph.wifi.bssid 02:00:00:00:00:00
```

Constraints

- Parameters related to GPS data and base station information

Table 5-1 GPS data

Parameter	Description	Mandatory	Default Value	Constraints
latitude	Specifies the latitude. The north latitude is positive and the south latitude is negative.	Yes	22.657501	Value range: –90.000000 to 90.000000 Unit: Degree (°)
longitude	Specifies the longitude The east longitude is positive and the west longitude is negative.	Yes	114.055939	Value range: –180.000000 to 180.000000 Unit: Degree (°)
altitude	Specifies the altitude.	No	51.0	Unit: Meter
speed	Specifies the speed.	No	0.0	Unit: Meter
bearing	Specifies the azimuth. 0° indicates due north, 90° indicates due east, 180° indicates due south, and 270° indicates due west.	No	30.0	Value range: 0.0 to 360.0 Unit: Degree (°)
accuracy	Specifies the positioning accuracy.	No	90.0	Unit: Meter

Table 5-2 Base station information

Parameter	Description	Mandatory	Constraints
cell_type	Specifies the base station type.	Yes	The type can **GSM**, **CDMA**, **WCDMA**, and **LTE**.

Parameter	Description	Mandatory	Constraints
mcc	Specifies the country code.	No	Example: 460
mnc	Specifies the mobile network code of a base station.	No	For Code-division multiple access (CDMA), only **system id** is available. **mnc** is used for injection.
lac	Specifies the area code of a base station.	Yes	For CDMA, only **network id** is available. **lac** is used for injection. For Long Term Evolution (LTE), only **tac** is available. **lac** is used for injection.
cid	Specifies the base station ID.	Yes	For CDMA, only **base station id** is available. **cid** is used for injection. For LTE, only **ci** is available. **cid** is used for injection.

- All characters are English characters.
- The World Geodetic System 1984 (WGS84) is used for GPS data.
- Both LocationManager **GPS_PROVIDER** and **NETWORK_PROVIDER** use the longitude and latitude information of the GPS.
- Geocoder that supports geocoding and reverse geocoding is supported only in the Chinese Mainland, Hong Kong, and Macao.
- The setting takes effect immediately.

5.12 App Installation Whitelist

Function

The App installation whitelist can be configured. If no whitelist is configured, any APK can be installed.

How to Use

Push the configuration file to the **/data/local/config/InstallWhitelist** path. If you want to set a whitelist for all applications of a series, you can use the substring shared by the package names of this series of applications in the configuration file. For example, company A launches two applications and their package names are com.aaa.bbb and com.aaa.ccc. If you want to set a whitelist for the packages of the two applications at the same time, you can configure **com.aaa** in the whitelist.

Constraints

- The configuration format must be as follows: ${partial_package_name}

Examples:

com.aaa

com.company1.package

com.company2.package

- The configuration file uses the Unix line feed (\n).
- Set the **/data/local/config** folder permissions to 755.
- Set the file permissions to 644.
- The setting takes effect immediately.

5.13 App Installation Blacklist

Function

Applications added to the blacklist cannot be installed. If you want to set a blacklist for all applications of a series, you can use the substring shared by the package names of this series of applications in the configuration file. For example, company A launches two applications and their package names are com.aaa.bbb and com.aaa.ccc. If you want to set a blacklist for the packages of the two applications at the same time, you can configure **com.aaa** in the whitelist.

How to Use

Push the configuration file to the **/data/local/config/InstallBlacklist** path.

Constraints

- The configuration format must be as follows: ${partial_package_name}

Examples:

com.aaa

com.company1.package

com.company2.package

- The configuration file uses the Unix line feed (\n).
- Set the **/data/local/config** folder permissions to 755.
- Set the file permissions to 644.
- The setting takes effect immediately.

5.14 Forcibly Installing a 32-Bit Application

Function

If both 32-bit and 64-bit APKs are supported, the 32-bit APK will be installed on the cloud phone.

How to Use

You push the configuration file to **/data/local/config/use32bit** and installs the APK. The 32-bit APK will be installed on the cloud phone. You can also delete the current configuration file, uninstall the 32-bit APK, and install the 64-bit APK.

Constraints

- If the configured APK does not support 32-bit, the application will fail to be installed.
- The configuration format is as follows: ${package_name}

  Examples:

  com.aaa.bbb

  com.aaa.ccc

  com.aaa.ddd
- The configuration file uses the Unix line feed (\n).
- Set the file permission to 644.
- The setting takes effect immediately.

5.15 Dynamically Changing the System Language

Function

Run the **am** command to dynamically change the system language.

How to Use

adb shell am update-config --locale *Language tags*

Constraints

- Language label of each country

  For details, see **Language Tags**. For the source code of the opn-source project, see **/aosp/frameworks/base/core/res/res/values/locale_config.xml**.
- Use commas (,) to separate multiple language tags.

  For example, to change the current language list to English+Chinese and configure English to the default language, run the following command:

  adb shell am update-config --locale en-US,zh-CN
- The setting takes effect immediately.

5.16 Background Process Management

Function

The cloud phone **performance** automatically clears background application processes. It prevents automatic startup and mutual wakeup of the third-party applications in the background. This improves the startup speed and reduces the occurrence of OOM and high CPU usage.

- **performance**: low-memory detection and process killing policy

  When the remaining memory of a cloud phone is lower than a threshold, processes with different priorities are killed in descending order of the remaining memory size.

Level	Remaining Memory	Processes to Be Cleared
High	25% of the total memory	Empty processes Cache processes
Middle	20% of the total memory	Used and unperceivable processes (invisible, no floating window, no audio focus, and more)
Low	15% of the total memory	Activity processes that have been used last time Provider processes that have been used last time Background service processes
Critical	200 MB	Kill all application processes in descending order of the memory used until the remaining memory is greater than 200 MB.

How to Use

- Listening to the broadcast of the killed application

  Your background management program obtains the package name and cause why the application was killed by listening to the broadcast of the killed application.

```
public static final String ACTION_APP_KILLED = "android.intent.action.APP_KILLED";

private MyBroadcastReceiver mBroadcastReceiver = new MyBroadcastReceiver();

private void registerReceiver() {
    IntentFilter filter = new IntentFilter(ACTION_APP_KILLED);
    this.registerReceiver(mBroadcastReceiver, filter);
}

private void unregisterReceiver() {
    this.unregisterReceiver(mBroadcastReceiver);
}

private class MyBroadcastReceiver extends BroadcastReceiver {

    private static final String TAG = "AppKilled";

    @Override
    public void onReceive(Context context, Intent intent) {
        Log.d(TAG, "package: " + intent.getStringExtra("package"));
```



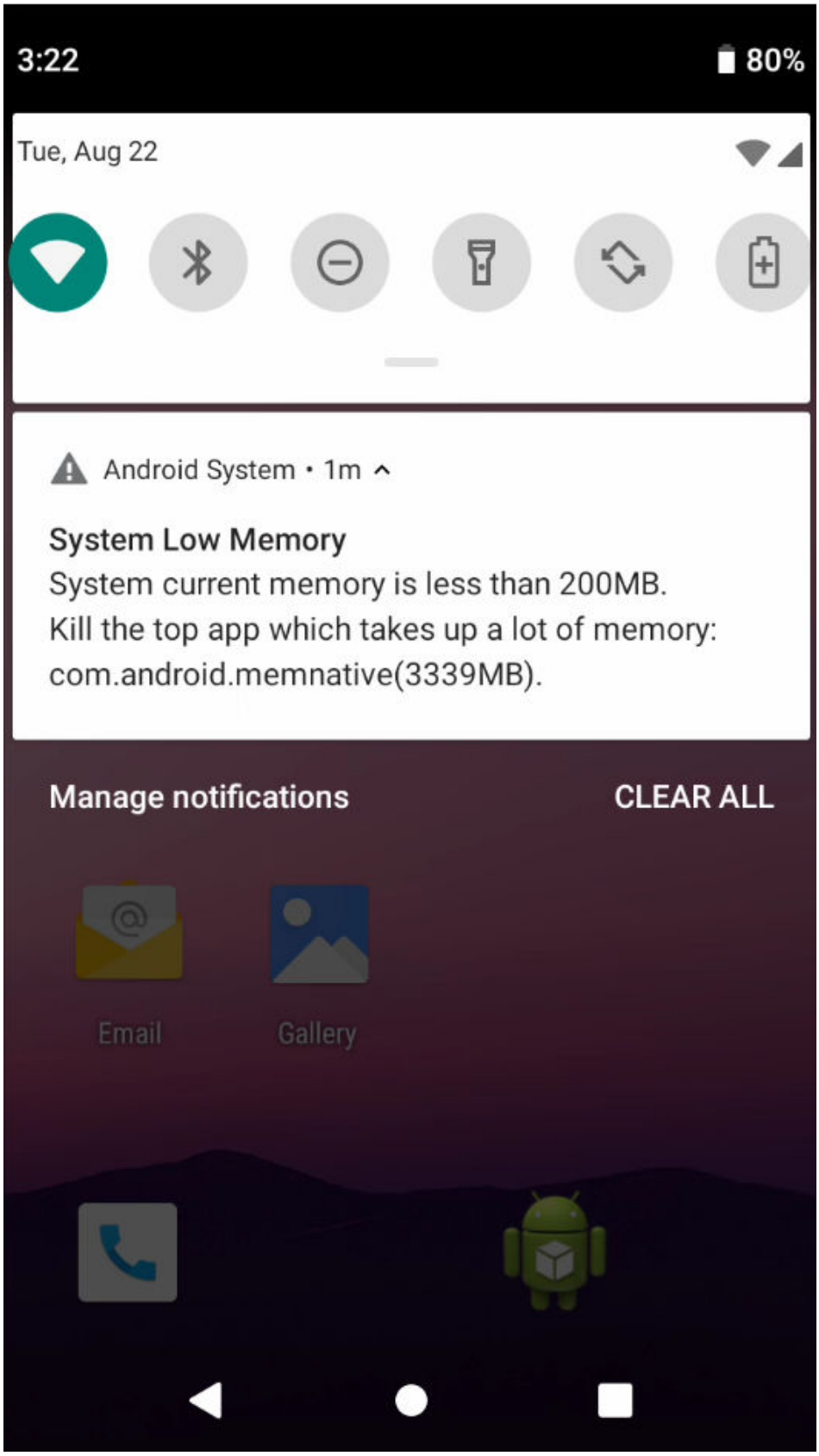
```
        Log.d(TAG, "reason: " + intent.getStringExtra("reason"));
    }
}
```

- Example of memory leak in the foreground app

  The total memory of a cloud phone is 3.79 GB. Compile the demo app to request ultra-large memory. Use the Java layer to call the native layer through the Java Native Interface (JNI) so that the remaining memory of the system is less than 200 MB. As a result, processes corresponding to the high level to the critical level are killed.

```
#define LOGI(...) __android_log_print(ANDROID_LOG_INFO,TAG,__VA_ARGS__)
#define LOGE(...) __android_log_print(ANDROID_LOG_ERROR,TAG,__VA_ARGS__)
extern "C" JNIEXPORT jint JNICALL
Java_com_android_memnative_MainActivity_mallocMem(JNIEnv *env, jobject thiz, jint mb) {
    jint total = 0;
    for (jint i = 0; i < mb; i++) {
        jint size = sizeof(char) * 1024 * 1024;
        char *p = (char *) malloc(size);
        if (p != NULL) {
            memset(p, 1, size);
            LOGI("malloc success: %d mb\n", mb);
            total += 1;
        } else {
            LOGE("malloc failed: %d mb\n", mb);
        }
    }
    LOGI("malloc total: %d mb\n", total);
    return total;
}
public class MainActivity extends AppCompatActivity {

    static {
        System.loadLibrary("memnative");
    }

    public native int mallocMem(int mb);

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        setContentView(R.layout.activity_main);

        mallocMem(3300); // malloc native memory 3300MB
    }
}
```

  The system automatically clears the application processes based on the process importance and sends a broadcast of the application killed. After the background processes are cleared, if the remaining memory is still less than 200 MB and there is a foreground app that uses the largest amount of memory, the foreground app will be killed and a low memory notification is displayed in the notification bar.



- Background automatic startup management policy

Except for the processes of the applications specified in the following exemption policies, third-party application processes are not allowed to automatically start or wake up each other in the background.

Application to Which Exemption Policies Apply	Example
System applications	/system/app, /system/priv-app, and more
Privileged applications	uid=1000 (system processes), the default input method, and more
Visualization applications	Apps with desktop widgets and live wallpapers
Whitelisted applications	Refer to the command line tool.

- Key Logcat logs
  - Key logs of low memory detection and process killing

    logcat | grep LMK

    ```
    BackgroundAppKiller: [LMK] start to kill top app, which takes up a lot of memory: ActivityRecord{248080f u0 com.android.memnative/.MainActivity t84}
    BackgroundAppKiller: [LMK] Killing AppInfo{packageName='com.android.memnative', uid=10059, isHighMemClean=false, reason='[memory:critical]', startTraffic=0, delayMillis=0, totalMillis=0}
    lowmemorykiller: [LMK] start to kill process.
    lowmemorykiller: [LMK] Killing 'com.android.deskclock' (4198), uid 10049, adj 906
    ```

    BackgroundAppKiller: **performance**

    lowmemorykiller: native AOSP low memory killer daemon (lmkd) service
  - Viewing logs of processes that are automatically started in the background and intercepted

    logcat -s AutoRunController | grep "has no auto-run permission"

    ```
    AutoRunController: com.android.memnative has no auto-run permission to startProcess
    ```

- Command line tool
  - **adb shell cmd performance** *[command] [args]*

    You can use this command to enable or disable a **performance** feature of CPH, add a whitelist, or delete a whitelist.

Command	Parameter	Description	Example
bg-killer	-e <true|false>	Enables or disables background process clearing. This feature is enabled by default.	adb shell cmd performance bg-killer -e true

Command	Parameter	Description	Example
	-a <packageName|packageNames>	Adds a whitelist of background processes to be cleared. Use commas (,) to separate multiple package names.	adb shell cmd performance bg-killer -a com.android.test1,com.android.test2
	-d <packageName|packageNames>	Deletes the whitelist of background processes to be cleared. Use commas (,) to separate multiple package names.	adb shell cmd performance bg-killer -d com.android.test1,com.android.test2
auto-run	-e <true|false>	Enables or disables automatic startup of background third-party applications. This feature is enabled by default.	adb shell cmd performance auto-run -e true
	-a <packageName|packageNames>	Adds a whitelist of third-party applications that will automatically start in the background. Use commas (,) to separate multiple package names.	adb shell cmd performance auto-run -a com.android.test1,com.android.test2

Command	Parameter	Description	Example
	-d <packageName| packageNames>	Deletes the whitelist of third-party applications that will automatically start in the background. Use commas (,) to separate multiple package names.	adb shell cmd performance auto-run -d com.android.test1,com.android.test2

- **adb shell dumpsys performance** *[command] [args]*

  You can use this command to view whether a **performance** feature of CPH is enabled or not and to view a whitelist.

Constraints

- Background process management is enabled by default.
- By default, daemon processes and processes of whitelisted applications are exempted.
- All running application processes, including those of the whitelisted applications, at the critical level of low memory, will be killed.

5.17 Texture Compression

Function

By default, texture compression is enabled on cloud phones to lower the GPU memory usage. CPH allows you to dynamically enable or disable texture compression by running commands.

How to Use

Run the following command to enable or disable texture compression:

```
adb shell cmd attributes texture-compression <enable/disable>
```

Run the following command to check whether texture compression is enabled:

```
adb shell cmd attributes list
```

Constraints

After enabling or disabling texture compression, restart applications for the setting to take effect.

Disabling texture compression may increase the GPU memory usage and cause your cloud phone to respond slowly, so you are advised not to disable texture compression.

5.18 Restarting a Cloud Phone

Function

You can restart a cloud phone within a cloud phone instead of restarting it on the management plane.

How to Use

NOTE

You'd better perform flow control when you restart cloud phones within them. That is because concurrent restart of a large number of cloud phones may cause a sudden surge in the load of the cloud phone server, which may affect other cloud phones that are running properly.

- Restarting a cloud phone through the CLI

  ```
  adb shell reboot
  ```

  Constraints: Only the process whose UID is 0, 1000, or 2000 has the permissions to run the **reboot** command.

- Restarting a cloud phone by calling the PowerManager API

  ```
  PowerManager powerManager = getSystemService(PowerManager.class);
  powerManager.reboot("your reason for reboot");
  ```

  Constraint: Only the process whose UID is 0 and 1000 has the permissions to invoke the PowerManager API.

- Restarting a cloud phone by injecting **keyevent --longpress KEYCODE_POWER**

  ```
  adb shell input keyevent --longpress KEYCODE_POWER
  ```

  After **keyevent --longpress KEYCODE_POWER** is injected, the restart option is displayed on the screen. After you click the button, the cloud phone restarts.

  The button UI may vary depending on the AOSP version.

  Constraints: Only the process whose UID is 0, 1000, or 2000 has the permissions to inject the press & hold power button.

6 Device Emulation

Function

The cloud phone does not have a physical camera, microphone, or sensor, but supports emulation of these devices, so that the cloud phone can better collaborate with the mobile phone.

If you want to know more about how to use these emulated devices, contact your account manager to obtain related documents.

Virtual Devices

- Virtual camera

  The audio and video interfaces on the cloud phone can be invoked to enable or disable the virtual camera, obtain camera information, and configure camera parameters.
- Virtual microphone

  The audio and video interfaces of the cloud phone can be invoked to enable the microphone and start recording, set recording parameters, and disable the microphone or recording.
- Virtual gyroscope

  The audio and video interfaces of the cloud phone can be invoked to inject sensor data and set the acceleration sensor and precision.

7 Cloud Phone Audio and Video

Function

The cloud phone provides an audio and video engine, allowing you to use the cloud phone to collect and encode audios and videos and flexibly configure audio and video encoding parameters to meet service requirements in different scenarios.

If you want to know more about how to use these functions, contact your account manager to obtain related documents.

Cloud Phone Audio

- Initializing the audio service

  Configures audio initialization parameters, including the audio type, sampling rate, sampling depth, and sampling interval.
- Starting the audio service

  Starts the audio service to obtain audio data.
- Stopping the audio service

  Stops obtaining audio data.
- Destroying the audio service

  Destroys the audio service.
- Obtaining the audio service status

  Obtains the audio service status, such as running, stopped, or invalid.
- Configuring audio parameters

  Configures audio parameters, including the audio type, sampling rate, sampling depth, and sampling interval.

Cloud Phone Video

- Initializing the video service

  Configures video initialization parameters, including the video format, encoding mode, resolution, and bit rate.
- Starting the video service

  Starts the video service to obtain video data.

- Stopping the video service

  Stops obtaining video data.
- Destroying the video service

  Destroys the video service.
- Obtaining the video service status

  Obtain the video service status, such as initializing, running, stopped, or invalid.
- Obtaining parameters of the current video service

  Obtains the current parameter configurations, such as the frame rate, bit rate, bit rate control mode, and resolution of the video service.
- Configuring video parameters dynamically

  Dynamically configures video service parameters, such as the frame rate, bit rate, and resolution.

Cloud Phone Touchscreen

- Touch injection

  The server receives and processes the control data.
- Key injection

  The server receives and processes the key operation data.
- Handle operation injection

  The server receives and processes the handle control data.
- Touch injection

  Stops touch injection.

8 Configuring a Route

You can configure routes to forward all outbound traffic of all cloud phones under your tenant to the selected VPC peering connection.

If you choose custom network when purchasing a cloud phone server, the server belongs to the VPC specified by the tenant. For details about how to configure routes, see **Creating a VPC Peering Connection with Another VPC in Your Account**.

CAUTION

Once the route is configured successfully, the next hop of the outbound traffic of all your cloud phones will be directly connected to the VPC peering connection. If your cloud phones want to access the Internet, you can only use a server in the VPC corresponding to the VPC peering connection you have selected.

Prerequisites

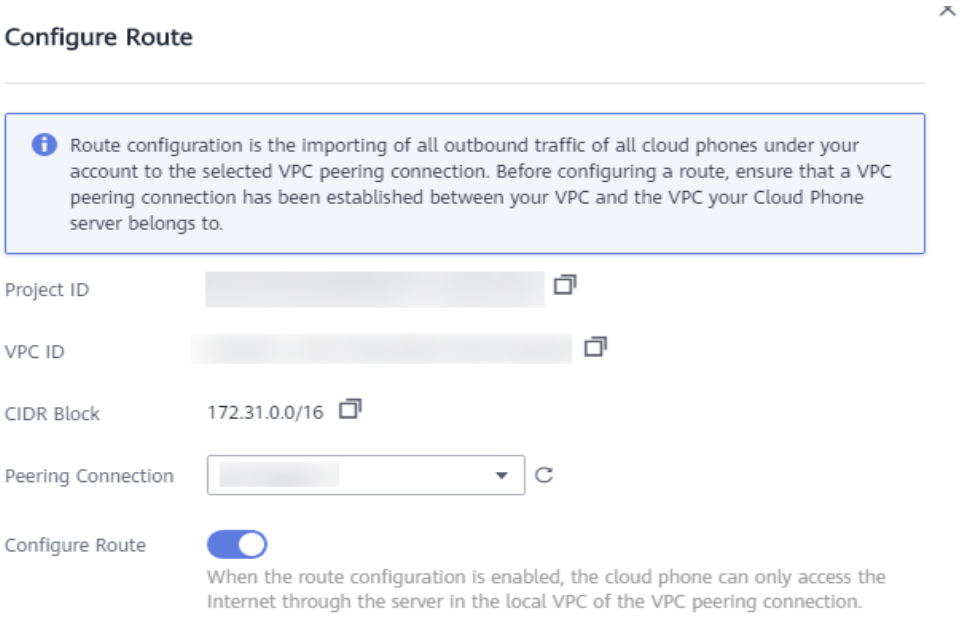
A VPC peering connection has been established between your VPC and the VPC which your server belongs to, and the connection status is **Accepted**. For details, see **Step 1: Create a VPC Peering Connection (Only When the Jump Server and the Cloud Phone Are in Different VPCs)**.

Procedure

1. Log in to the management console.
2. In the upper left corner, select the target region.
3. On the **Service List** page, choose **Compute** > **Cloud Phone Host**.

   The CPH console is displayed.
4. In the navigation pane on the left, choose **Servers**.
5. In the upper part of the server list, click **Configure Route**.
6. In the right pane, select a VPC peering connection, enable **Configure Route**, and click **OK**.

Figure 8-1 Configure Route



Execution Result

After the routing function is enabled, the cloud phone traffic will be transmitted through the VPC peering connection.

9 Permission Management

9.1 Creating a User and Granting CPH Permissions

This section describes how to use **IAM** to implement fine-grained permissions control for your CPH resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing cloud resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust a Huawei Cloud account or cloud service to perform efficient O&M on your CPH resources.

If your Huawei Cloud account does not need individual IAM users, skip this chapter.

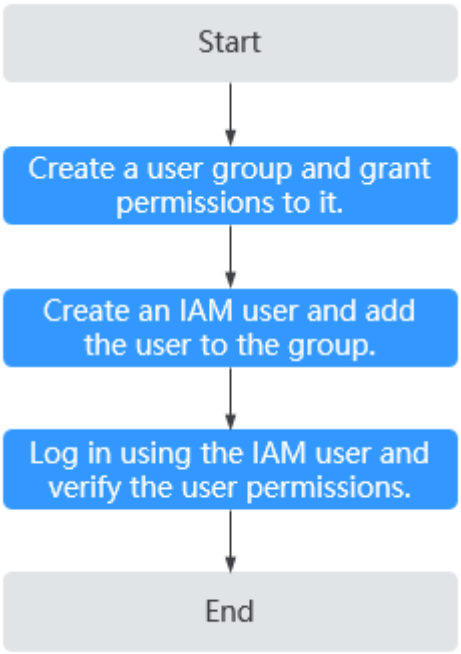
This section uses the **CPH User** policy as an example to describe how to grant permissions to a user. **Figure 9-1** shows the process.

Prerequisites

Learn about the permissions (see **Permissions Management**) supported by CPH and choose policies or roles according to your requirements. For the system policies of other services, see **System-defined Permissions**.

Authorization Process

Figure 9-1 Process for granting CPH permissions



1. **Create a user group and assign permissions** to it.

   On the IAM console, create a user group, and assign the read-only permission **CPH User** and its dependent permission **Tenant Guest** to the group.

2. **Create an IAM user and add it to the user group**.

   Create a user on the IAM console and add the user to the group created in step **1**.

3. **Log in** and verify permissions.

   Log in to the management console as the created user, switch to the authorized region, and verify that the user has the required permissions. (Assume that the user has only the CPH User and Tenant Guest permissions.)

   - Click **Service List**. Choose **Compute** > **Cloud Phone Host**. In the navigation pane on the left, choose **Servers** and **Instances** to view the server data and cloud phone data respectively. If the cloud phone information can be viewed, the read-only permission has taken effect.
   - Click **Service List**. Choose **Compute** > **Cloud Phone Host**. On the displayed CPH console, check whether the **Buy Server** button is displayed in the upper right corner. If no, the read-only permission has taken effect.

9.2 Permission Configuration Examples

You can select roles and policies to grant permissions. This section provides common permission configuration examples. For details, see **Creating a User and Granting CPH Permissions**.

Examples of permission configurations:

- **Granting All Permissions**
- **Granting Operation Permissions**
- **Granting Read-Only Permissions**
- **Granting Permissions to Perform Specified Operations**

Granting All Permissions

If you grant the all permissions of CPH to IAM users, grant the **CPH FullAccess** and **DEW KeypairFullAccess** policies and set custom policies for viewing, paying, and renewing orders. **Figure 9-2** shows how to create a custom policy. For details about how to create a custom policy, see **Creating a Custom Policy**. **Figure 9-3** shows how to grant all permissions of CPH.

Custom policy

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "bss:renewal:update",
            "bss:balance:view",
            "bss:order:view",
            "bss:order:pay",
            "bss:order:update",
            "bss:renewal:view"
         ]
      }
   ]
}
```

Figure 9-2 All permissions-custom policy

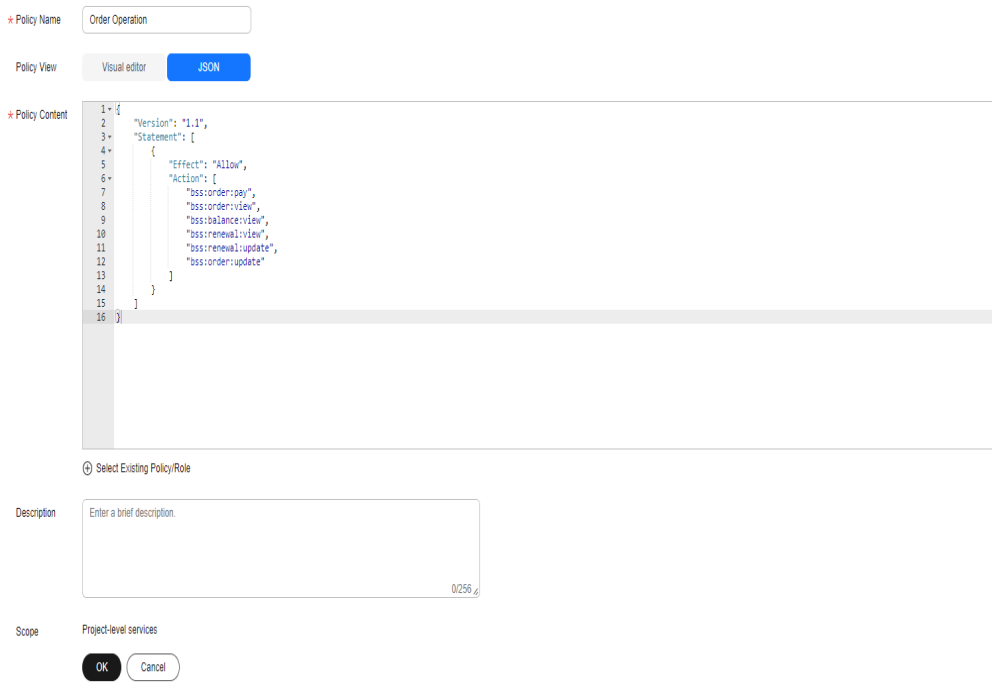
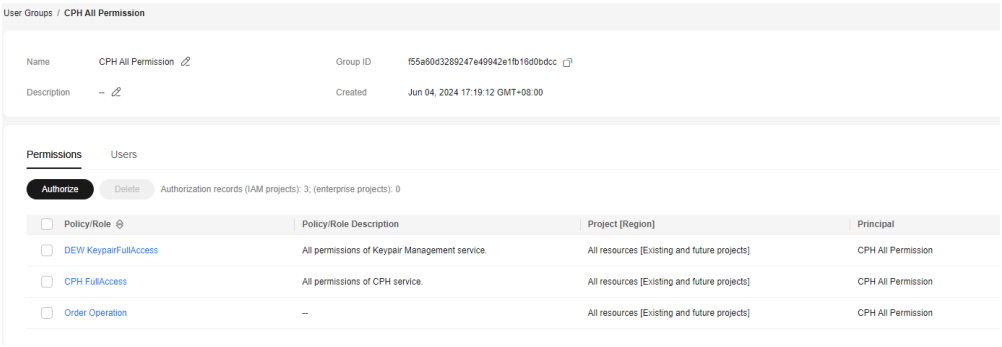


Figure 9-3 Granting all permissions of CPH



Granting Operation Permissions

Operation permissions allow IAM users to operate but not to create or delete cloud phone servers or cloud phones. To grant the CPH operation permissions to IAM users, grant the **CPH FullAccess** policy and set a custom policy that denies the **create** and **delete** action. **Figure 9-4** shows how to create a custom policy. For details about how to create a custom policy, see **Creating a Custom Policy**. **Figure 9-5** shows how to grant the operation permissions.

Custom policy

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Deny ",
         "Action": [
            "cph:servers:create ",
            "cph:servers:delete "
         ]
      }
   ]
}
```

Figure 9-4 Operation permissions-custom policy

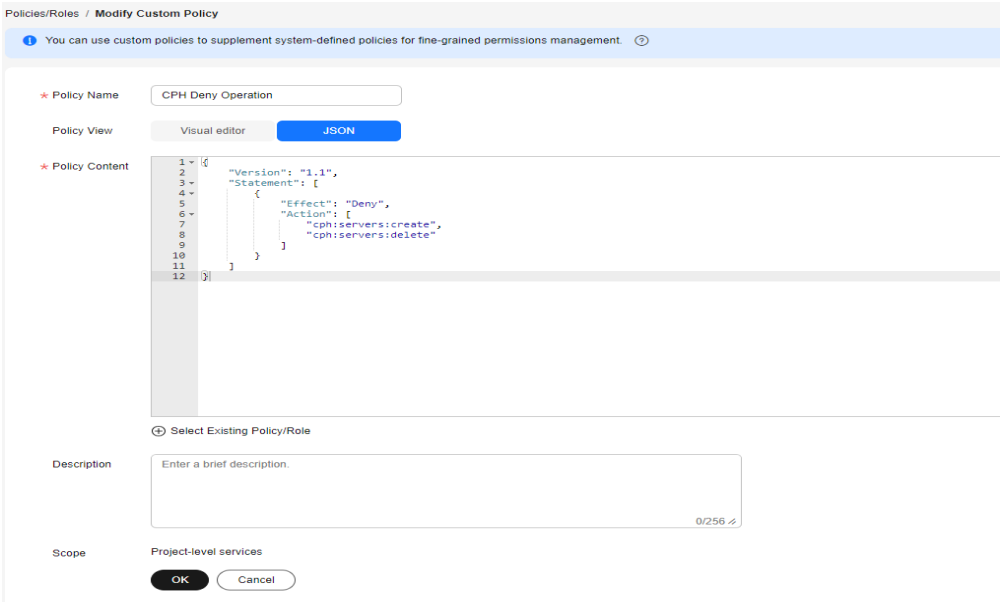
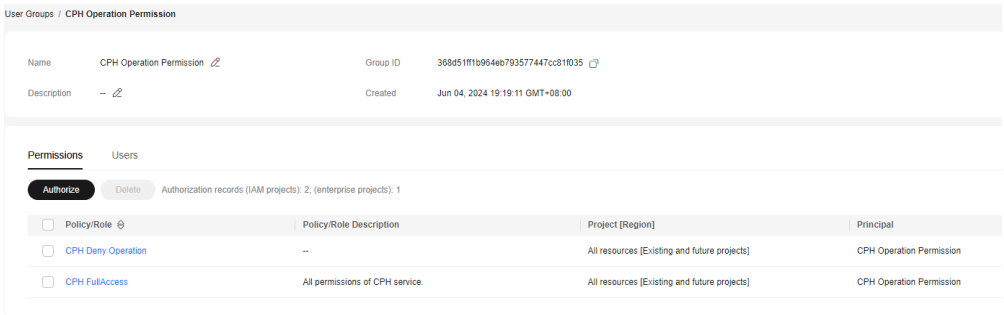


Figure 9-5 Granting operation permissions



Granting Read-Only Permissions

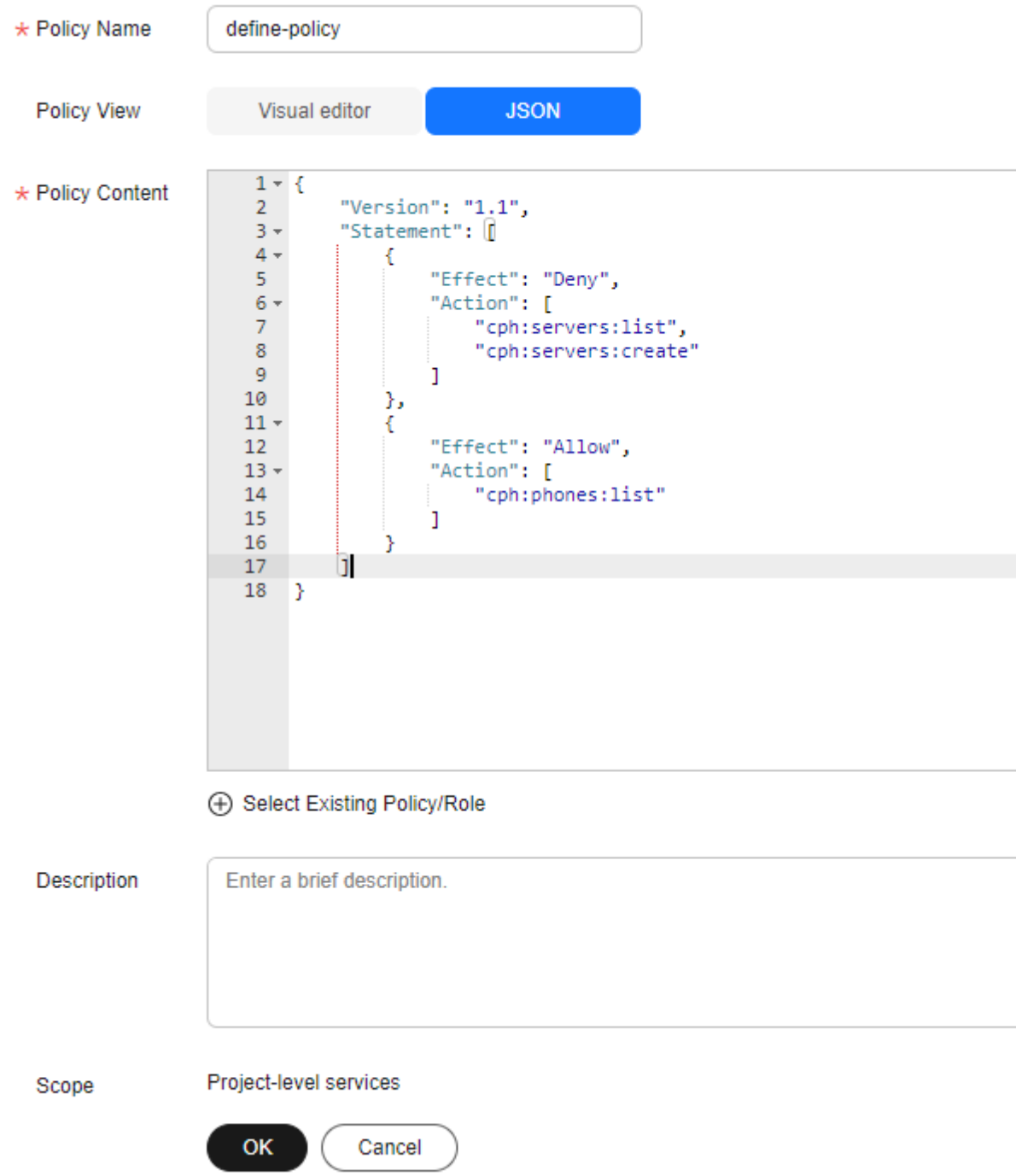
To grant the CPH read-only permissions to IAM users, authorize the **ReadOnlyAccess** policy.

Figure 9-6 Granting read-only permissions

Granting Permissions to Perform Specified Operations

To grant an IAM user the permissions to perform specified operations on CPH, create a custom policy to allow or deny specified operations. **Figure 9-7** shows how to create a custom policy. For details about how to create a custom policy, see **Creating a Custom Policy**.

Figure 9-7 Creating a custom policy to allow or deny specified operations



10 Adjusting Resource Quotas

What Is a Quota?

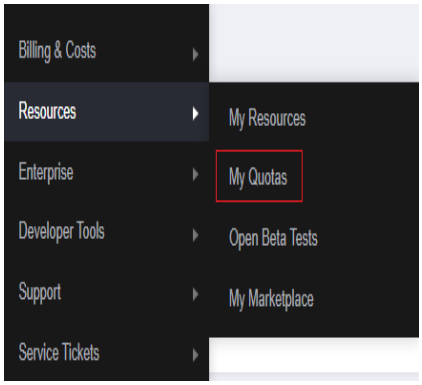
Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number and capacity of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

If the existing resource quota cannot meet your requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources** > **My Quotas**.
   The **Service Quota** page is displayed.

   Figure 10-1 My Quotas

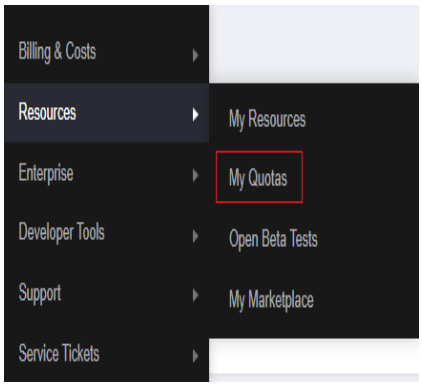
   

4. View the used and total quota of each type of resources on the displayed page.
   If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

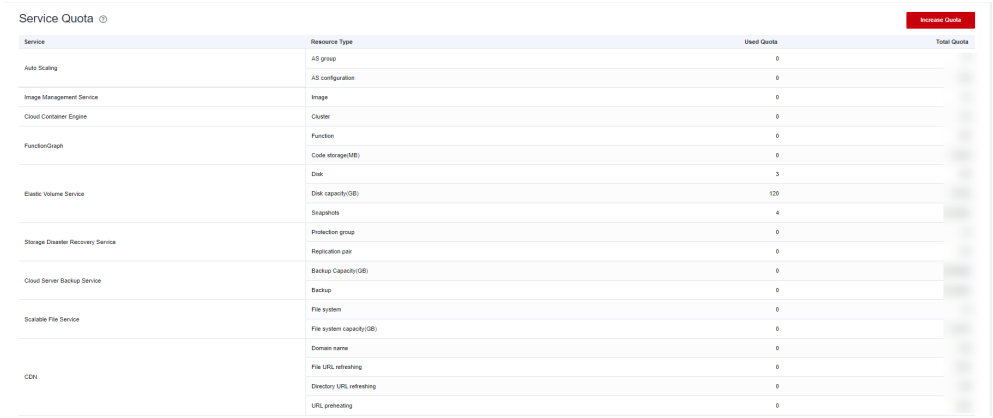
1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources** > **My Quotas**.
   The **Service Quota** page is displayed.

   Figure 10-2 My Quotas

3. Click **Increase Quota** in the upper right corner of the page.

   Figure 10-3 Increasing quota

4. On the **Create Service Ticket** page, configure parameters as required.
   In the **Problem Description** area, fill in the content and reason for adjustment.
5. After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.

11 Monitoring

11.1 Supported Metrics

This topic describes monitored metrics reported by CPH to Cloud Eye as well as their namespace and dimensions. You can log in to the Cloud Eye **console** or call the Cloud Eye **APIs** to query the metrics of the monitored objects and alarms generated for CPH.

Namespace

SYS.CPH

Metrics

CPH supports the following metrics: cloud phone server metrics (**Table 11-1**), cloud phone metrics (**Table 11-2**), disk metrics (**Table 11-3**), and GPU metrics (**Table 11-4**).

Table 11-1 Cloud phone server metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
cpu_usage	CPU Usage	CPU usage of the monitored server	0–100%	Cloud phone server	1 minute
load_average5	5-Minute Avg. Load	CPU load averaged for the last 5 minutes for the monitored server	≥ 0	Cloud phone server	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mem_usedPercent	Memory Usage	Memory usage of the monitored server	0–100%	Cloud phone server	1 minute
net_rx	Network Rate (Incoming)	Bytes/second received by all NICs of the monitored server	≥ 0 bytes/s	Cloud phone server	1 minute
net_tx	Network Rate (Outgoing)	Bytes/second sent by all NICs of the monitored server	≥ 0 bytes/s	Cloud phone server	1 minute
cph_sharebase_usedPercent	Shared Storage Usage	Shared storage used by the monitored server	0–100%	Cloud phone server	1 minute

Table 11-2 Cloud phone metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
cph_cpu_usage	CPU Usage	Cloud phone CPU usage	0–100%	Cloud phone	1 minute
cph_mem_usedPercent	Memory Usage	Cloud phone memory usage (%)	0–100%	Cloud phone	1 minute
cph_mem_used	Memory Used	Cloud phone memory used (bytes)	> 0 bytes	Cloud phone	1 minute
cph_net_rx	Network Rate (Incoming)	Bytes/second received by the cloud phone NIC	≥ 0 bytes/s	Cloud phone	1 minute
cph_net_tx	Network Rate (Outgoing)	Bytes/second sent by the cloud phone NIC	≥ 0 bytes/s	Cloud phone	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
cph_disk_agt_read_bytes_rate	I/O Read Rate	Bytes read from the cloud phone per second	≥ 0 bytes/s	Cloud phone	1 minute
cph_disk_agt_write_bytes_rate	I/O Write Rate	Bytes written to the cloud phone per second	≥ 0 bytes/s	Cloud phone	1 minute
cph_disk_usedPercent	Disk Usage	Cloud phone disk usage	0–100%	Cloud phone	1 minute
cph_disk_percent	Data Disk Usage	Data disk usage of the cloud phone	0–100%	Cloud phone	1 minute
cph_disk_inode_percent	Data Disk inode Usage	Data disk inode usage of the cloud phone	0–100%	Cloud phone	1 minute
cph_sysdisk_percent	System Disk Usage	System disk usage of the cloud phone	0–100%	Cloud phone	1 minute
cph_sysdisk_inode_percent	System Disk inode Usage	System inode disk usage of the cloud phone	0–100%	Cloud phone	1 minute
cph_gpu_mem	GPU Memory Size	Total GPU memory size (MB) of the cloud phone	≥ 0 MB	Cloud phone	1 minute

Table 11-3 Disk metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
disk_usage_read_request_rate	Disk Read IOPS	Read requests/second sent to the monitored disk	≥ 0 requests/s	Disk	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
disk_usage_write_request_rate	Disk Write IOPS	Write requests/second sent to the monitored disk per second	≥ 0 requests/s	Disk	1 minute
disk_usage_read_rate	Disk Read Bandwidth	KB/second read from the monitored disk	≥ 0 KB/s	Disk	1 minute
disk_usage_write_rate	Disk Write Bandwidth	KB/second written to the monitored disk	≥ 0 KB/s	Disk	1 minute
disk_usage_read_await	Disk Read Await	Average wait time per I/O read for the monitored disk in the monitoring period	≥ 0 ms/operation	Disk	1 minute
disk_usage_write_await	Disk Write Await	Average wait time per I/O write for the monitored disk in the monitoring period	≥ 0 ms/operation	Disk	1 minute
disk_usage_svctm	Disk I/O Service Time	Average service time per I/O read or write for the monitored disk in the monitoring period	≥ 0 ms	Disk	1 minute
disk_usage_util	Disk I/O Utilization	Percentage of time spent during which read and write requests were sent to the monitored disk in the monitoring period	0–100%	Disk	1 minute

Table 11-4 GPU metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
gpu_usage_gpu_load	GPU Usage	GPU usage of the monitored video card on the server	0–100%	Cloud phone server	1 minute
gpu_usage_vram	GPU VRAM Usage	GPU VRAM usage of the monitored video card on the server	0–100%	Cloud phone server	1 minute
gpu_usage_gtt	GPU GTT Usage	GPU GTT usage of the monitored video card on the server	0–100%	Cloud phone server	1 minute
gpu_usage_power	GPU Power	GPU power of the monitored video card on the server	> 0 W	Cloud phone server	1 minute
gpu_usage_temperature	GPU Temperature	GPU temperature of the monitored video card on the server	> 0℃	Cloud phone server	1 minute
gpu_usage_status	GPU Status	GPU status of the monitored video card on the server	N/A	Cloud phone server	1 minute
gpu_mem_busy_percent	GPU Memory Load	GPU memory load of the cloud phone	0–100%	GPU	1 minute

Dimensions

Key	Value
instance_id	Cloud phone server ID
cph_id	Cloud phone ID
disk_name	Disk name
gpu_index	GPU name

11.2 CPH Events

Table 11-5 CPH events

Event Source	Event Name	Event ID	Alarm Severity	Description	Solution	Impact
CPH	GPU failure	gpuAbnormal	Critical	The GPU was faulty.	GPU faults can be handled in the following ways: • **hard_hang**: Hardware was faulty. Submit a service ticket. • **over_temp**: The graphics card temperature exceeded the upper limit. Submit a service ticket. • **lost_card**: The graphics card was missing. Submit a service ticket. • **light_reset_success**: The lightweight reset of the graphics card was successful, which may cause artifacts on the cloud phone. Restart the cloud phone. • **deep_reset_success**: The heavyweight reset of the graphics card was successful, which may cause artifacts on some cloud phones connected to this graphics card. Reset the graphics card or submit a service ticket. • **deep_reset_failed**: The heavyweight reset of the graphics card failed. Restart the server to restore services, or submit a service ticket.	Services are interrupted.

Event Source	Event Name	Event ID	Alarm Severity	Description	Solution	Impact
					• **fan_damaged**: The fan is damaged and the graphics card must be replaced. Submit a service ticket.	
	GPU back to normal	gpuNormal	Informational	The GPU was running properly.	No further action is required.	N/A
	Kernel crash	gpuNormal	Critical	The kernel log indicated **crash**.	Submit a service ticket.	Services are interrupted during the crash.
	Kernel OOM	kernelOom	Major	The kernel log indicated **out of memory**.	Submit a service ticket.	Services are interrupted.
	Hardware malfunction	hardwareError	Critical	The kernel log indicated **Hardware Error**.	Submit a service ticket.	Services are interrupted.
	PCIe error	pcieAer	Critical	The kernel log indicated **PCIE Bus Error**.	Submit a service ticket.	Services are interrupted.
	SCSI error	scsiError	Critical	The kernel log indicated **SCSI error**.	Submit a service ticket.	Services are interrupted.

Event Source	Event Name	Event ID	Alarm Severity	Description	Solution	Impact
	Image storage became read-only	partReadOnly	Critical	The image storage became read-only.	Submit a service ticket.	Services are interrupted.
	Image storage superblock damaged	badSuperBlock	Critical	The superblock of the file system of the image storage was damaged.	Submit a service ticket.	Services are interrupted.
	Image storage /.sharedpath/master became read-only	isuladMasterReadOnly	Critical	Mount point /.sharedpath/master of the image storage became read-only.	Submit a service ticket.	Services are interrupted.
	Cloud phone data disk became read-only	cphDiskReadOnly	Critical	The cloud phone data disk became read-only.	Submit a service ticket.	Services are interrupted.

Event Source	Event Name	Event ID	Alarm Severity	Description	Solution	Impact
	Cloud phone data disk superblock damaged	cphDiskReadOnly	Critical	The superblock of the file system of the cloud phone data disk was damaged.	Submit a service ticket.	Services are interrupted.

11.3 Viewing CPH Metrics

This topic describes how to view the metrics of a cloud phone server, cloud phone, disk, or GPU.

Procedure

1. Log in to the management console.
2. In the upper left corner, select the target region.
3. Click **Service List**. Under **Management & Governance**, click **Cloud Eye**.
4. In the navigation pane on the left, choose **Cloud Service Monitoring** > **Cloud Phone Host**.
5. Select a server and click **View Metric** in the **Operation** column.
6. Go back to the cloud phone server list, click ⌄ to expand a server, and view monitoring information about the cloud phones, GPUs, and disks.

11.4 Creating an Alarm Rule

This topic describes how to create an alarm rule. You can create alarm rules and configure alarm notifications to learn about the usages and statuses of cloud phone servers, cloud phones, disks, and GPUs in a timely manner.

Procedure

1. Log in to the management console.
2. In the upper left corner, select the target region.
3. Click **Service List**. Under **Management & Governance**, click **Cloud Eye**.

4. In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.
5. On the displayed **Alarm Rules** page, click **Create Alarm Rule**.
   - **Resource Type**: indicates the name of the service for which the alarm rule is configured. Select **Cloud Phone Host**.
   - **Dimension**: The dimension can be **Cloud Phone Servers**, **Cloud Phone Servers - Cloud Phones**, **Cloud Phone Servers - Disks**, or **Cloud Phone Servers - GPUs**. Configure this parameter as required.

   For details about other parameters, see **Creating an Alarm Rule**.
6. Click **Create Now**.

   If you have enabled **Alarm Notification**, you will be notified when an alarm is triggered.

12 CTS

12.1 Key Cloud Phone Operations Recorded by CTS

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.

With CTS, you can record operations associated with CPH for later query, audit, and backtrack operations.

Prerequisites

Enable CTS before using it. If CTS is not enabled, resource operations cannot be recorded. After CTS is enabled, CTS automatically creates a tracker and records all operations of the current tenant in the tracker. CTS traces of the last seven days can be displayed at most. To save operation records for a long time, you can store trace files in OBS buckets. For details, see **Enabling CTS**.

Key Cloud Phone Operations

Table 12-1 Cloud phone operations that can be recorded by CTS

Operation	Resource	Trace Name
Buying a cloud phone	phone	createCloudPhone
Updating the cloud phone name	phone	updatePhoneName
Resetting a cloud phone	phone	resetCloudPhone
Restarting a cloud phone	phone	restartCloudPhone
Adding SD card files	phone	addSdFiles

Operation	Resource	Trace Name
Deleting SD card files	phone	deleteSdFiles
Setting event notification	phone	setEventNotification

12.2 Viewing Traces

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in OBS buckets. CTS stores operation records generated in the last seven days.

This section describes how to query and export operation records of the last seven days on the CTS console.

- **Viewing Real-Time Traces in the Trace List of the New Edition**
- **Viewing Real-Time Traces in the Trace List of the Old Edition**

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for more than seven days, you must configure an OBS bucket to transfer records to it. Otherwise, you cannot query the operation records generated seven days ago.
- After performing operations on the cloud, you can query management traces on the CTS console 1 minute later and query data traces on the CTS console 5 minutes later.

Viewing Real-Time Traces in the Trace List of the New Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
   - **Trace Name**: Enter a trace name.
   - **Trace ID**: Enter a trace ID.
   - **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API

operation does not involve the resource name parameter, leave this field empty.

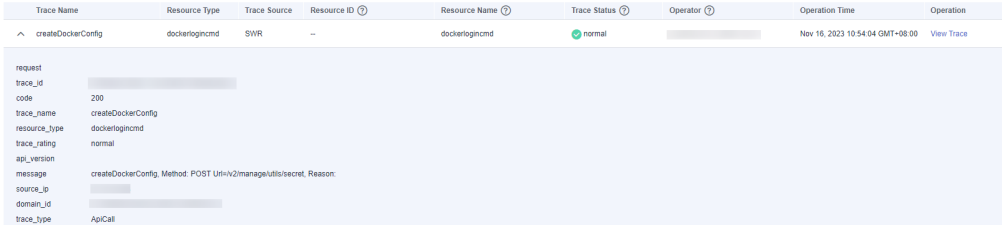
- **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
- **Trace Source**: Select a cloud service name from the drop-down list.
- **Resource Type**: Select a resource type from the drop-down list.
- **Operator**: Select one or more operators from the drop-down list.
- **Trace Status**: Select **normal**, **warning**, or **incident**.
  - **normal**: The operation succeeded.
  - **warning**: The operation failed.
  - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
- **Enterprise Project ID**: Enter an enterprise project ID.
- **Access Key**: Enter an access key ID, including temporary access credentials and permanent access keys.
- Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.

5. On the **Trace List** page, you can also export and refresh the trace list, and customize the list display settings.
   - Enter any keyword in the search box and press Enter to filter desired traces.
   - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5000 records.
   - Click  to view the latest information about traces.
   - Click  to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled (), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

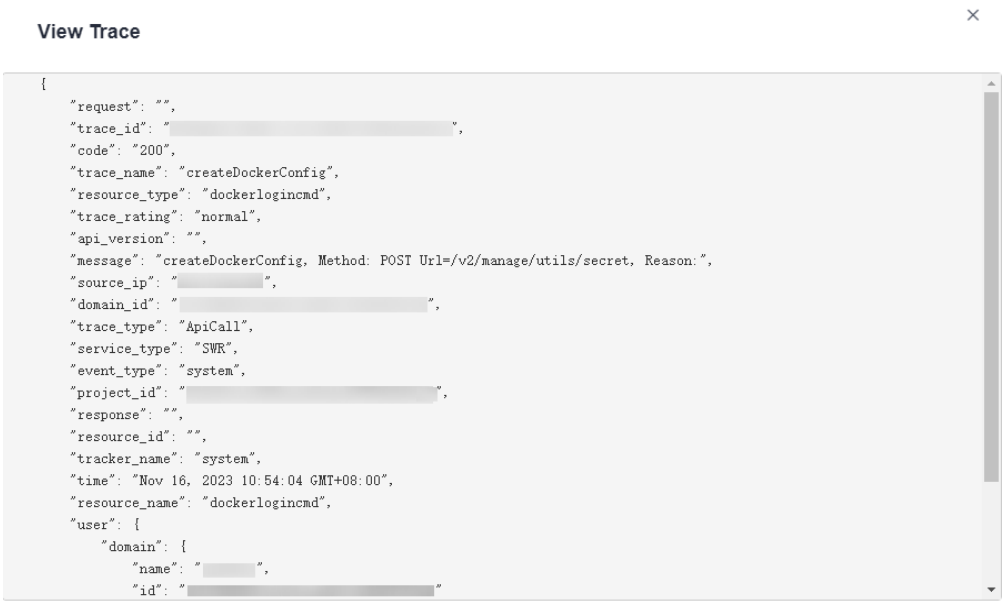
Viewing Real-Time Traces in the Trace List of the Old Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.

5. Set filters to search for your desired traces. The following filters are available:
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
     - If you select **Resource ID** for **Search By**, specify a resource ID.
     - If you select **Trace name** for **Search By**, specify a trace name.
     - If you select **Resource name** for **Search By**, specify a resource name.
   - **Operator**: Select a user.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: You can query traces generated during any time range in the last seven days.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
   - Click to view the latest information about traces.
8. Click on the left of a trace to expand its details.



9. Click **View Trace** in the **Operation** column. The trace details are displayed.



10. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces** in the *CTS User Guide*.

11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

13 Appendix

13.1 Language Tags

Table 13-1 Language tags

Language Tag	Language (Country/Region)
af-NA	Afrikaans (Namibia)
af-ZA	Afrikaans (South Africa)
agq-CM	Aghem (Cameroon)
ak-GH	Akan (Ghana)
am-ET	Amharic (Ethiopia)
ar-AE	Arabic (United Arab Emirates)
ar-AE-u-nu-latn	Arabic (United Arab Emirates,Western Digits)
ar-BH	Arabic (Bahrain)
ar-BH-u-nu-latn	Arabic (Bahrain,Western Digits)
ar-DJ	Arabic (Djibouti)
ar-DJ-u-nu-latn	Arabic (Djibouti,Western Digits)
ar-DZ	Arabic (Algeria)
ar-DZ-u-nu-arab	Arabic (Algeria,Arabic-Indic Digits)
ar-EG	Arabic (Egypt)
ar-EG-u-nu-latn	Arabic (Egypt,Western Digits)
ar-EH	Arabic (Western Sahara)
ar-EH-u-nu-arab	Arabic (Western Sahara,Arabic-Indic Digits)

Language Tag	Language (Country/Region)
ar-ER	Arabic (Eritrea)
ar-ER-u-nu-latn	Arabic (Eritrea,Western Digits)
ar-IL	Arabic (Israel)
ar-IL-u-nu-latn	Arabic (Israel,Western Digits)
ar-IQ	Arabic (Iraq)
ar-IQ-u-nu-latn	Arabic (Iraq,Western Digits)
ar-JO	Arabic (Jordan)
ar-JO-u-nu-latn	Arabic (Jordan,Western Digits)
ar-KM	Arabic (Comoros)
ar-KM-u-nu-latn	Arabic (Comoros,Western Digits)
ar-KW	Arabic (Kuwait)
ar-KW-u-nu-latn	Arabic (Kuwait,Western Digits)
ar-LB	Arabic (Lebanon)
ar-LB-u-nu-latn	Arabic (Lebanon,Western Digits)
ar-LY	Arabic (Libya)
ar-LY-u-nu-arab	Arabic (Libya,Arabic-Indic Digits)
ar-MA	Arabic (Morocco)
ar-MA-u-nu-arab	Arabic (Morocco,Arabic-Indic Digits)
ar-MR	Arabic (Mauritania)
ar-MR-u-nu-latn	Arabic (Mauritania,Western Digits)
ar-OM	Arabic (Oman)
ar-OM-u-nu-latn	Arabic (Oman,Western Digits)
ar-PS	Arabic (Palestine)
ar-PS-u-nu-latn	Arabic (Palestine,Western Digits)
ar-QA	Arabic (Qatar)
ar-QA-u-nu-latn	Arabic (Qatar,Western Digits)
ar-SA	Arabic (Saudi Arabia)
ar-SA-u-nu-latn	Arabic (Saudi Arabia,Western Digits)
ar-SD	Arabic (Sudan)
ar-SD-u-nu-latn	Arabic (Sudan,Western Digits)

Language Tag	Language (Country/Region)
ar-SO	Arabic (Somalia)
ar-SO-u-nu-latn	Arabic (Somalia,Western Digits)
ar-SS	Arabic (South Sudan)
ar-SS-u-nu-latn	Arabic (South Sudan,Western Digits)
ar-SY	Arabic (Syria)
ar-SY-u-nu-latn	Arabic (Syria,Western Digits)
ar-TD	Arabic (Chad)
ar-TD-u-nu-latn	Arabic (Chad,Western Digits)
ar-TN	Arabic (Tunisia)
ar-TN-u-nu-arab	Arabic (Tunisia,Arabic-Indic Digits)
ar-XB	Right-to-left pseudolocale
ar-YE	Arabic (Yemen)
ar-YE-u-nu-latn	Arabic (Yemen,Western Digits)
as-IN	Assamese (India)
asa-TZ	Asu (Tanzania)
az-Cyrl-AZ	Azerbaijani (Cyrillic,Azerbaijan)
az-Latn-AZ	Azerbaijani (Latin,Azerbaijan)
bas-CM	Basaa (Cameroon)
be-BY	Belarusian (Belarus)
bem-ZM	Bemba (Zambia)
bez-TZ	Bena (Tanzania)
bg-BG	Bulgarian (Bulgaria)
bm-ML	Bambara (Mali)
bn-BD	Bengali (Bangladesh)
bn-BD-u-nu-latn	Bengali (Bangladesh,Western Digits)
bn-IN	Bengali (India)
bn-IN-u-nu-latn	Bengali (India,Western Digits)
bo-CN	Tibetan (China)
bo-IN	Tibetan (India)
br-FR	Breton (France)

Language Tag	Language (Country/Region)
brx-IN	Bodo (India)
bs-Cyrl-BA	Bosnian (Cyrillic,Bosnia & Herzegovina)
bs-Latn-BA	Bosnian (Latin,Bosnia & Herzegovina)
ca-AD	Catalan (Andorra)
ca-ES	Catalan (Spain)
ca-FR	Catalan (France)
ca-IT	Catalan (Italy)
ce-RU	Chechen (Russia)
cgg-UG	Chiga (Uganda)
chr-US	Cherokee (United States)
cs-CZ	Czech (Czechia)
cy-GB	Welsh (United Kingdom)
da-DK	Danish (Denmark)
da-GL	Danish (Greenland)
dav-KE	Taita (Kenya)
de-AT	German (Austria)
de-BE	German (Belgium)
de-CH	German (Switzerland)
de-DE	German (Germany)
de-LI	German (Liechtenstein)
de-LU	German (Luxembourg)
dje-NE	Zarma (Niger)
dsb-DE	Lower Sorbian (Germany)
dua-CM	Duala (Cameroon)
dyo-SN	Jola-Fonyi (Senegal)
dz-BT	Dzongkha (Bhutan)
ebu-KE	Embu (Kenya)
ee-GH	Ewe (Ghana)
ee-TG	Ewe (Togo)
el-CY	Greek (Cyprus)

Language Tag	Language (Country/Region)
el-GR	Greek (Greece)
en-AG	English (Antigua & Barbuda)
en-AI	English (Anguilla)
en-AS	English (American Samoa)
en-AT	English (Austria)
en-AU	English (Australia)
en-BB	English (Barbados)
en-BE	English (Belgium)
en-BI	English (Burundi)
en-BM	English (Bermuda)
en-BS	English (Bahamas)
en-BW	English (Botswana)
en-BZ	English (Belize)
en-CA	English (Canada)
en-CC	English (Cocos (Keeling) Islands)
en-CH	English (Switzerland)
en-CK	English (Cook Islands)
en-CM	English (Cameroon)
en-CX	English (Christmas Island)
en-CY	English (Cyprus)
en-DE	English (Germany)
en-DG	English (Diego Garcia)
en-DK	English (Denmark)
en-DM	English (Dominica)
en-ER	English (Eritrea)
en-FI	English (Finland)
en-FJ	English (Fiji)
en-FK	English (Falkland Islands (Islas Malvinas))
en-FM	English (Micronesia)
en-GB	English (United Kingdom)

Language Tag	Language (Country/Region)
en-GD	English (Grenada)
en-GG	English (Guernsey)
en-GH	English (Ghana)
en-GI	English (Gibraltar)
en-GM	English (Gambia)
en-GU	English (Guam)
en-GY	English (Guyana)
en-HK	English (Hong Kong)
en-IE	English (Ireland)
en-IL	English (Israel)
en-IM	English (Isle of Man)
en-IN	English (India)
en-IO	English (British Indian Ocean Territory)
en-JE	English (Jersey)
en-JM	English (Jamaica)
en-KE	English (Kenya)
en-KI	English (Kiribati)
en-KN	English (St. Kitts & Nevis)
en-KY	English (Cayman Islands)
en-LC	English (St. Lucia)
en-LR	English (Liberia)
en-LS	English (Lesotho)
en-MG	English (Madagascar)
en-MH	English (Marshall Islands)
en-MO	English (Macau)
en-MP	English (Northern Mariana Islands)
en-MS	English (Montserrat)
en-MT	English (Malta)
en-MU	English (Mauritius)
en-MW	English (Malawi)

Language Tag	Language (Country/Region)
en-MY	English (Malaysia)
en-NA	English (Namibia)
en-NF	English (Norfolk Island)
en-NG	English (Nigeria)
en-NL	English (Netherlands)
en-NR	English (Nauru)
en-NU	English (Niue)
en-NZ	English (New Zealand)
en-PG	English (Papua New Guinea)
en-PH	English (Philippines)
en-PK	English (Pakistan)
en-PN	English (Pitcairn Islands)
en-PR	English (Puerto Rico)
en-PW	English (Palau)
en-RW	English (Rwanda)
en-SB	English (Solomon Islands)
en-SC	English (Seychelles)
en-SD	English (Sudan)
en-SE	English (Sweden)
en-SG	English (Singapore)
en-SH	English (St. Helena)
en-SI	English (Slovenia)
en-SL	English (Sierra Leone)
en-SS	English (South Sudan)
en-SX	English (Sint Maarten)
en-SZ	English (Swaziland)
en-TC	English (Turks & Caicos Islands)
en-TK	English (Tokelau)
en-TO	English (Tonga)
en-TT	English (Trinidad & Tobago)

Language Tag	Language (Country/Region)
en-TV	English (Tuvalu)
en-TZ	English (Tanzania)
en-UG	English (Uganda)
en-UM	English (U.S. Outlying Islands)
en-US	English (United States)
en-VC	English (St. Vincent & Grenadines)
en-VG	English (British Virgin Islands)
en-VI	English (U.S. Virgin Islands)
en-VU	English (Vanuatu)
en-WS	English (Samoa)
en-XA	Left-to-right pseudolocale
en-ZA	English (South Africa)
en-ZM	English (Zambia)
en-ZW	English (Zimbabwe)
es-AR	Spanish (Argentina)
es-BO	Spanish (Bolivia)
es-CL	Spanish (Chile)
es-CO	Spanish (Colombia)
es-CR	Spanish (Costa Rica)
es-CU	Spanish (Cuba)
es-DO	Spanish (Dominican Republic)
es-EA	Spanish (Ceuta & Melilla)
es-EC	Spanish (Ecuador)
es-ES	Spanish (Spain)
es-GQ	Spanish (Equatorial Guinea)
es-GT	Spanish (Guatemala)
es-HN	Spanish (Honduras)
es-IC	Spanish (Canary Islands)
es-MX	Spanish (Mexico)
es-NI	Spanish (Nicaragua)

Language Tag	Language (Country/Region)
es-PA	Spanish (Panama)
es-PE	Spanish (Peru)
es-PH	Spanish (Philippines)
es-PR	Spanish (Puerto Rico)
es-PY	Spanish (Paraguay)
es-SV	Spanish (El Salvador)
es-US	Spanish (United States)
es-UY	Spanish (Uruguay)
es-VE	Spanish (Venezuela)
et-EE	Estonian (Estonia)
eu-ES	Basque (Spain)
ewo-CM	Ewondo (Cameroon)
fa-AF	Persian (Afghanistan)
fa-AF-u-nu-latn	Persian (Afghanistan,Western Digits)
fa-IR	Persian (Iran)
fa-IR-u-nu-latn	Persian (Iran,Western Digits)
ff-CM	Fulah (Cameroon)
ff-GN	Fulah (Guinea)
ff-MR	Fulah (Mauritania)
ff-SN	Fulah (Senegal)
fi-FI	Finnish (Finland)
fil-PH	Filipino (Philippines)
fo-DK	Faroese (Denmark)
fo-FO	Faroese (Faroe Islands)
fr-BE	French (Belgium)
fr-BF	French (Burkina Faso)
fr-BI	French (Burundi)
fr-BJ	French (Benin)
fr-BL	French (St. Barthélemy)
fr-CA	French (Canada)

Language Tag	Language (Country/Region)
fr-CD	French (Congo (DRC))
fr-CF	French (Central African Republic)
fr-CG	French (Congo (Republic))
fr-CH	French (Switzerland)
fr-CI	French (Côte d'Ivoire)
fr-CM	French (Cameroon)
fr-DJ	French (Djibouti)
fr-DZ	French (Algeria)
fr-FR	French (France)
fr-GA	French (Gabon)
fr-GF	French (French Guiana)
fr-GN	French (Guinea)
fr-GP	French (Guadeloupe)
fr-GQ	French (Equatorial Guinea)
fr-HT	French (Haiti)
fr-KM	French (Comoros)
fr-LU	French (Luxembourg)
fr-MA	French (Morocco)
fr-MC	French (Monaco)
fr-MF	French (St. Martin)
fr-MG	French (Madagascar)
fr-ML	French (Mali)
fr-MQ	French (Martinique)
fr-MR	French (Mauritania)
fr-MU	French (Mauritius)
fr-NC	French (New Caledonia)
fr-NE	French (Niger)
fr-PF	French (French Polynesia)
fr-PM	French (St. Pierre & Miquelon)
fr-RE	French (Réunion)

Language Tag	Language (Country/Region)
fr-RW	French (Rwanda)
fr-SC	French (Seychelles)
fr-SN	French (Senegal)
fr-SY	French (Syria)
fr-TD	French (Chad)
fr-TG	French (Togo)
fr-TN	French (Tunisia)
fr-VU	French (Vanuatu)
fr-WF	French (Wallis & Futuna)
fr-YT	French (Mayotte)
fur-IT	Friulian (Italy)
fy-NL	Western Frisian (Netherlands)
ga-IE	Irish (Ireland)
gd-GB	Scottish Gaelic (United Kingdom)
gl-ES	Galician (Spain)
gsw-CH	Swiss German (Switzerland)
gsw-FR	Swiss German (France)
gsw-LI	Swiss German (Liechtenstein)
gu-IN	Gujarati (India)
guz-KE	Gusii (Kenya)
gv-IM	Manx (Isle of Man)
ha-GH	Hausa (Ghana)
ha-NE	Hausa (Niger)
ha-NG	Hausa (Nigeria)
haw-US	Hawaiian (United States)
iw-IL	Hebrew (Israel)
hi-IN	Hindi (India)
hr-BA	Croatian (Bosnia & Herzegovina)
hr-HR	Croatian (Croatia)
hsb-DE	Upper Sorbian (Germany)

Language Tag	Language (Country/Region)
hu-HU	Hungarian (Hungary)
hy-AM	Armenian (Armenia)
in-ID	Indonesian (Indonesia)
ig-NG	Igbo (Nigeria)
ii-CN	Sichuan Yi (China)
is-IS	Icelandic (Iceland)
it-CH	Italian (Switzerland)
it-IT	Italian (Italy)
it-SM	Italian (San Marino)
ja-JP	Japanese (Japan)
jgo-CM	Ngomba (Cameroon)
jmc-TZ	Machame (Tanzania)
ka-GE	Georgian (Georgia)
kab-DZ	Kabyle (Algeria)
kam-KE	Kamba (Kenya)
kde-TZ	Makonde (Tanzania)
kea-CV	Kabuverdianu (Cape Verde)
khq-ML	Koyra Chiini (Mali)
ki-KE	Kikuyu (Kenya)
kk-KZ	Kazakh (Kazakhstan)
kkj-CM	Kako (Cameroon)
kl-GL	Kalaallisut (Greenland)
kln-KE	Kalenjin (Kenya)
km-KH	Khmer (Cambodia)
kn-IN	Kannada (India)
ko-KP	Korean (North Korea)
ko-KR	Korean (South Korea)
kok-IN	Konkani (India)
ksb-TZ	Shambala (Tanzania)
ksf-CM	Bafia (Cameroon)

Language Tag	Language (Country/Region)
ksh-DE	Colognian (Germany)
kw-GB	Cornish (United Kingdom)
ky-KG	Kyrgyz (Kyrgyzstan)
lag-TZ	Langi (Tanzania)
lb-LU	Luxembourgish (Luxembourg)
lg-UG	Ganda (Uganda)
lkt-US	Lakota (United States)
ln-AO	Lingala (Angola)
ln-CD	Lingala (Congo (DRC))
ln-CF	Lingala (Central African Republic)
ln-CG	Lingala (Congo (Republic))
lo-LA	Lao (Laos)
lt-LT	Lithuanian (Lithuania)
lu-CD	Luba-Katanga (Congo (DRC))
luo-KE	Luo (Kenya)
luy-KE	Luyia (Kenya)
lv-LV	Latvian (Latvia)
mas-KE	Masai (Kenya)
mas-TZ	Masai (Tanzania)
mer-KE	Meru (Kenya)
mfe-MU	Morisyen (Mauritius)
mg-MG	Malagasy (Madagascar)
mgh-MZ	Makhuwa-Meetto (Mozambique)
mgo-CM	Meta (Cameroon)
mk-MK	Macedonian (Macedonia (FYROM))
ml-IN	Malayalam (India)
mn-MN	Mongolian (Mongolia)
mr-IN	Marathi (India)
ms-BN	Malay (Brunei)
ms-MY	Malay (Malaysia)

Language Tag	Language (Country/Region)
ms-SG	Malay (Singapore)
mt-MT	Maltese (Malta)
my-MM	Burmese (Myanmar (Burma))
my-MM-u-nu-latn	Burmese (Myanmar (Burma), Western Digits)
mzn-IR	Mazanderani (Iran)
naq-NA	Nama (Namibia)
nb-NO	Norwegian Bokmål (Norway)
nb-SJ	Norwegian Bokmål (Svalbard & Jan Mayen)
nd-ZW	North Ndebele (Zimbabwe)
ne-IN	Nepali (India)
ne-NP	Nepali (Nepal)
nl-AW	Dutch (Aruba)
nl-BE	Dutch (Belgium)
nl-BQ	Dutch (Caribbean Netherlands)
nl-CW	Dutch (Curaçao)
nl-NL	Dutch (Netherlands)
nl-SR	Dutch (Suriname)
nl-SX	Dutch (Sint Maarten)
nn-NO	Norwegian Nynorsk (Norway)
nnh-CM	Ngiemboon (Cameroon)
nus-SS	Nuer (South Sudan)
nyn-UG	Nyankole (Uganda)
om-ET	Oromo (Ethiopia)
om-KE	Oromo (Kenya)
or-IN	Oriya (India)
os-GE	Ossetic (Georgia)
os-RU	Ossetic (Russia)
pa-Arab-PK	Punjabi (Arabic,Pakistan)
pa-Guru-IN	Punjabi (Gurmukhi,India)
pl-PL	Polish (Poland)

Language Tag	Language (Country/Region)
ps-AF	Pashto (Afghanistan)
pt-AO	Portuguese (Angola)
pt-BR	Portuguese (Brazil)
pt-CV	Portuguese (Cape Verde)
pt-GW	Portuguese (Guinea-Bissau)
pt-MO	Portuguese (Macau)
pt-MZ	Portuguese (Mozambique)
pt-PT	Portuguese (Portugal)
pt-ST	Portuguese (São Tomé & Príncipe)
pt-TL	Portuguese (Timor-Leste)
qu-BO	Quechua (Bolivia)
qu-EC	Quechua (Ecuador)
qu-PE	Quechua (Peru)
rm-CH	Romansh (Switzerland)
rn-BI	Rundi (Burundi)
ro-MD	Romanian (Moldova)
ro-RO	Romanian (Romania)
rof-TZ	Rombo (Tanzania)
ru-BY	Russian (Belarus)
ru-KG	Russian (Kyrgyzstan)
ru-KZ	Russian (Kazakhstan)
ru-MD	Russian (Moldova)
ru-RU	Russian (Russia)
ru-UA	Russian (Ukraine)
rw-RW	Kinyarwanda (Rwanda)
rwk-TZ	Rwa (Tanzania)
sah-RU	Sakha (Russia)
saq-KE	Samburu (Kenya)
sbp-TZ	Sangu (Tanzania)
se-FI	Northern Sami (Finland)

Language Tag	Language (Country/Region)
se-NO	Northern Sami (Norway)
se-SE	Northern Sami (Sweden)
seh-MZ	Sena (Mozambique)
ses-ML	Koyraboro Senni (Mali)
sg-CF	Sango (Central African Republic)
si-LK	Sinhala (Sri Lanka)
sk-SK	Slovak (Slovakia)
sl-SI	Slovenian (Slovenia)
smn-FI	Inari Sami (Finland)
sn-ZW	Shona (Zimbabwe)
so-DJ	Somali (Djibouti)
so-ET	Somali (Ethiopia)
so-KE	Somali (Kenya)
so-SO	Somali (Somalia)
sq-AL	Albanian (Albania)
sq-MK	Albanian (Macedonia (FYROM))
sq-XK	Albanian (Kosovo)
sr-Cyrl-BA	Serbian (Cyrillic,Bosnia & Herzegovina)
sr-Cyrl-ME	Serbian (Cyrillic,Montenegro)
sr-Cyrl-RS	Serbian (Cyrillic,Serbia)
sr-Cyrl-XK	Serbian (Cyrillic,Kosovo)
sr-Latn-BA	Serbian (Latin,Bosnia & Herzegovina)
sr-Latn-ME	Serbian (Latin,Montenegro)
sr-Latn-RS	Serbian (Latin,Serbia)
sr-Latn-XK	Serbian (Latin,Kosovo)
sv-AX	Swedish (Åland Islands)
sv-FI	Swedish (Finland)
sv-SE	Swedish (Sweden)
sw-CD	Swahili (Congo (DRC))
sw-KE	Swahili (Kenya)

Language Tag	Language (Country/Region)
sw-TZ	Swahili (Tanzania)
sw-UG	Swahili (Uganda)
ta-IN	Tamil (India)
ta-LK	Tamil (Sri Lanka)
ta-MY	Tamil (Malaysia)
ta-SG	Tamil (Singapore)
te-IN	Telugu (India)
teo-KE	Teso (Kenya)
teo-UG	Teso (Uganda)
th-TH	Thai (Thailand)
to-TO	Tongan (Tonga)
tr-CY	Turkish (Cyprus)
tr-TR	Turkish (Turkey)
twq-NE	Tasawaq (Niger)
tzm-MA	Central Atlas Tamazight (Morocco)
ug-CN	Uyghur (China)
uk-UA	Ukrainian (Ukraine)
ur-IN	Urdu (India)
ur-IN-u-nu-latn	Urdu (India,Western Digits)
ur-PK	Urdu (Pakistan)
ur-PK-u-nu-arabext	Urdu (Pakistan,Extended Arabic-Indic Digits)
uz-Arab-AF	Uzbek (Arabic,Afghanistan)
uz-Cyrl-UZ	Uzbek (Cyrillic,Uzbekistan)
uz-Latn-UZ	Uzbek (Latin,Uzbekistan)
vi-VN	Vietnamese (Vietnam)
vun-TZ	Vunjo (Tanzania)
wae-CH	Walser (Switzerland)
xog-UG	Soga (Uganda)
yav-CM	Yangben (Cameroon)
yo-BJ	Yoruba (Benin)

Language Tag	Language (Country/Region)
yo-NG	Yoruba (Nigeria)
yue-HK	Cantonese (Hong Kong)
zgh-MA	Standard Moroccan Tamazight (Morocco)
zh-Hans-CN	Chinese (Simplified Han,China)
zh-Hans-HK	Chinese (Simplified Han,Hong Kong)
zh-Hans-MO	Chinese (Simplified Han,Macau)
zh-Hans-SG	Chinese (Simplified Han,Singapore)
zh-Hant-HK	Chinese (Traditional Han,Hong Kong)
zh-Hant-MO	Chinese (Traditional Han,Macau)
zh-Hant-TW	Chinese (Traditional Han,Taiwan)
zu-ZA	Zulu (South Africa)

