Cloud Phone

User Guide

Issue	11
Date	2021-09-30

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.

Contents

1 Buying a Cloud Phone (with Detailed Parameter Description)

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**.
3. In the navigation pane on the left, choose **Servers**. In the upper right corner, click **Buy Server**.
4. Complete the basic configuration as prompted.

Table 1-1 Parameter description

Parameter	Description	Example Value
Billing Mode	Servers are billed only yearly/monthly.	Yearly/Monthly
Region	Cloud phones in different regions cannot communicate with each other over an intranet. For lower network latency and quicker resource access, select the nearest region. After a server is purchases, its region cannot be changed.	CN East-Shanghai1

Parameter	Description	Example Value
AZ	An AZ is a part of a region with its own independent power supplies and networks. AZs are physically isolated but can communicate through an internal network. • If you require high availability, buy servers in difference 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 **Specifications**.	Cloud phone server physical.rx1.xlarge
Instance Specifications	Set this parameter as required.	rx1.cp.c60.d10.e1v1
Phone Image	Only the Android OS is supported.	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 as prompted.

   Network customization has been available in the CN Southwest-Guiyang1 region. You are advised to use this function.

   physical.rx1 servers do not support network customization. **Table 1-3** shows their system-defined network configuration.

   NOTE

   Cloud phone network can be configured in the following two ways:

   - Custom network: You can reuse the existing VPCs to manage cloud phone servers and reuse resources such as the shared bandwidth that you have purchased. This function is only available in the Southwest-Guiyang1 region.
   - Default network: The system automatically creates VPCs and configures bandwidths for your cloud phone servers. The existing VPCs and bandwidths cannot be reused.

Table 1-2 Custom network configuration

Parameter	Description	Example Value
Networking	Set **Network** by selecting an available VPC and subnet from the drop-down list and specifying a private IP address assignment mode. Cloud phones use networks provided by a VPC, including subnets and security groups. Select an existing VPC or create one.	None
Security Group Authorization	A **cph_admin_trust** agency will be created for you. This agency has the **VPC FullAccess** permission. To authorize the Cloud Phone service to create an agency for you, ensure that your login user has the **Security Administrator** permission or the fine-grained permission **iam:agencies:createAgency** for creating agencies. For more information, see **Permission Management**. The Cloud Phone service will use the agency to perform the following operations: • Create an elastic NIC, EIP, and virtual IP address for a general-purpose or gaming cloud phone. • Create a default security group for the general-purpose or gaming cloud phone server and set the port range for the security group. The port range will be mapped to that of each cloud phone so that the instance can open application access ports. **NOTE** By default, if an ECS and 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 the instructions provided in **What Are the Security Group Authorization Rules for Cloud Phones Using Custom Networks?**	None
EIP	• **Auto assign**: Buy a new EIP for the cloud phone.	Buy now

Parameter	Description	Example Value
Line	• 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 provides automatic failover and chooses the optimal path when a network connection fails.	Dynamic BGP
Bandwidth	• **Dedicated**: You will be charged based on the total traffic you generate. • **Shared**: The bandwidth can be shared by multiple EIPs.	Shared
Bandwidth Size	Supported range: 1 Mbits/s to 2000 Mbit/s	300 Mbit/s
Bandwidth Name	If you set **Bandwidth** to **Shared**, select an existing shared bandwidth name from the drop-down list.	bandwidth-001

Table 1-3 Default network configuration

Parameter	Description	Example Value
Bandwidth Type	• **Dedicated**: Specifies the bandwidth used exclusively by each purchased server. Dedicated bandwidth is required for transmitting heavy data traffic. • **Shared**: Specifies the bandwidth shared by multiple servers of a user. Shared bandwidth can help reduce the cost of public network bandwidth. It is suitable for services where traffic peaks tend to be staggered.	Shared
Method	The method can be **Using existing** or **Create Shared Bandwidth**. If you use a shared bandwidth for the first time, select **Create Shared Bandwidth**.	Create Shared Bandwidth

Parameter	Description	Example Value
Billed By	The dedicated bandwidth is billed only by traffic, and the shared bandwidth is billed only by bandwidth. • **Traffic**: You specify a maximum bandwidth and pay for the total traffic you generate. • **Bandwidth**: You are charged based on the bandwidth size and usage duration. This price is not included in the price of a server.	Bandwidth
Bandwidth	Specifies the maximum bandwidth, which is fixed at **300 Mbit/s**.	300 Mbit/s
Bandwidth Name	• If you set **Method** to **Using existing**, select an existing shared bandwidth name from the drop-down list. The number of associated servers is displayed on the existing shared bandwidth, so you can choose the right one as needed. • If you set **Method** to **Create Shared Bandwidth**, enter the shared bandwidth name in the text box.	whole-bandwidth-xxxx
Bandwidth Size	This parameter is mandatory when you set **Method** to **Create Shared Bandwidth**. The larger the bandwidth, the higher the price. Set this parameter based on your service requirements.	5 Mbit/s

NOTE

The default network (VPC and bandwidth) configured in this step is used only by the Cloud Phone servers. The network details are not displayed on the **Network Console**.

6. Click **Next: Configure Advanced Settings**. Complete the advanced configuration as prompted.

Table 1-4 Parameter description

Parameter	Description	Example Value
Name	Specifies the name for the server and the cloud phones that are virtualized from the server. The name must be unique. 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 the ascending order. For example, if you purchased a server for virtualizing 60 cloud phones and entered **CPH** for **Name**, the server name is **CPH-1**, and the cloud phone names range from **CPH-1-00001** to **CPH-1-00060**.	CPH
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 has been created, you can click **Create Key Pair** to create a key pair. Go back to the **Configure Advanced Settings** page, refresh the drop-down list, and select the created key pair. The private key 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 **Creating a Key Pair**.	KeyPair-test
VNC Login	After this function is enabled, you can log in to your cloud phone using VNC. **NOTE** Cloud phones of certain specifications do not support this function. For details about the cloud phones that support this function, see **What Are the Cloud Phone Specifications that Support VNC Login?**	N/A

Parameter	Description	Example Value
Application Port	This parameter is available when you select **Application Port** for **Advanced Settings**. Select this parameter when your cloud phones need to provide services for external systems. • **Application name**: The name can contain letters. However, the values **ADB** and **VNC** 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. That is, the cloud phone port and the server port are exposed to the Internet. – If this option is not selected, the cloud phone can be accessed only over the Intranet. **CAUTION** • Ensure that security control has been performed before you select **Internet access**. • The Cloud Phone service does not perform security check for the ports you configured for Internet access.	key 10001 Do not select it.

7. Click **Next: Confirm** to check the order.
   - If the information 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

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

  All cloud phones share a public IP address of the server. Each cloud phone has an independent private IP address.

- To access a cloud phone, use ADB or VNC. ADB is a common connection method and is supported by cloud phones of all specifications. VNC may not be supported by cloud phones of certain specifications. For details about the supported specifications, see **What Are the Specifications of Cloud Phones That Support VNC Login?**

  For details about the access methods, see **Access Methods**.
- After accessing your cloud phone, you may want to try some advanced functions. For details, visit the following links:

  Using Airtest to Quickly Obtain the Cloud Phone Screens

  Modifying the Cloud Phone GPS Location

  Using Cloud Phones to Build a Cloud Mobile Gaming System
- 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 or VNC.

- 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.
- VNC is a type of software used for screen sharing and remote operation. Through the network, the software can send the keyboard and mouse operations and real-time screens. This method is applicable to scenarios like smart game assistance and game trial.

Comparison Between the Two Access Methods

Table 2-1 Comparison

EIP	Screen/CLI Control	Requirement	Login Method
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 a HUAWEI CLOUD ECS as a jump server to access the cloud phone.	**ADB (Intranet)**

EIP	Screen/CLI Control	Requirement	Login Method
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.	None	**ADB (Recommended)** **ADB (Internet)**
Not required	Control the cloud phone on the cloud phone screen.	• The cloud phone specifications must be rx1.cp.c60.d32.e1v1.qemu. • **VNC login** in **Configure Advanced Settings** must be enabled during the server purchase.	**VNC (Intranet)**
Required one EIP for the server.	Control the cloud phone on the cloud phone screen.	• The cloud phone specifications must be rx1.cp.c60.d32.e1v1.qemu. • **VNC login** in **Configure Advanced Settings** must be enabled during the server purchase.	**VNC (Internet)**

2.2 ADB (Recommended)

You can use ADB to access your cloud phones on the Cloud Phone 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 **Computing** > **Cloud Phone**.
   The Cloud Phone 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**, and **7** in the lower part of the right panel, the command is automatically filled in the blank area. You only need to 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

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

   - **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?**

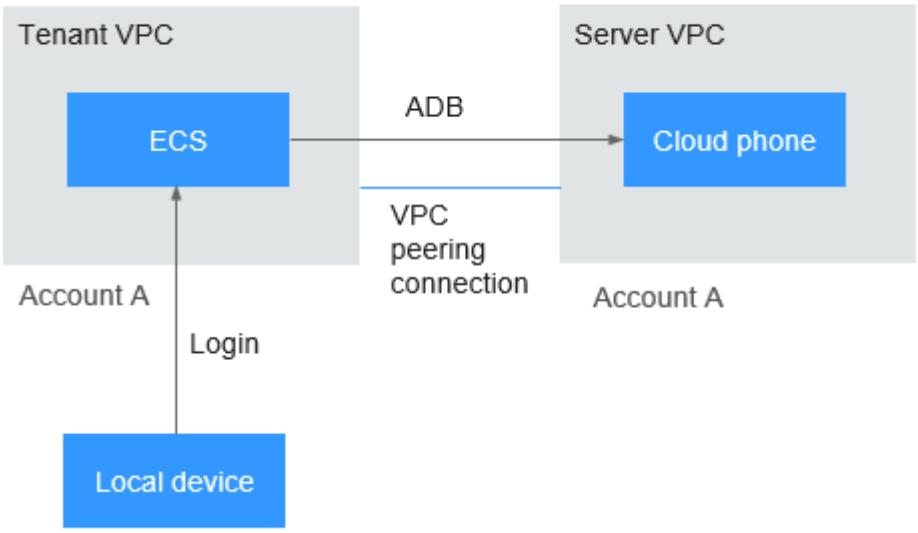
Helpful Links

- **Displaying the Cloud Phone Screens**
- **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 OS. This topic uses the Linux OS as an example.

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



Constraints and Limitations

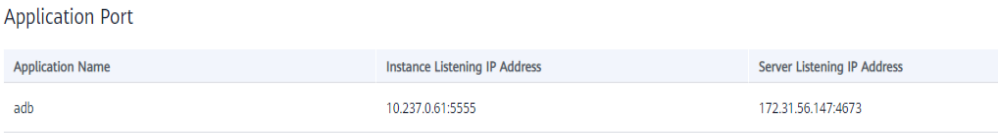
- You cannot establish a peering connection between the VPC of a tenant who has not purchased a server with the VPC where a purchased server is located. For example, in **Figure 2-1**, the tenant VPC and the VPC where the server resides belong to account A. A VPC peering connection across accounts cannot 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 the details page of the cloud phone and obtain the server listening address in the **Application Port** area.

Figure 2-2 Application Port



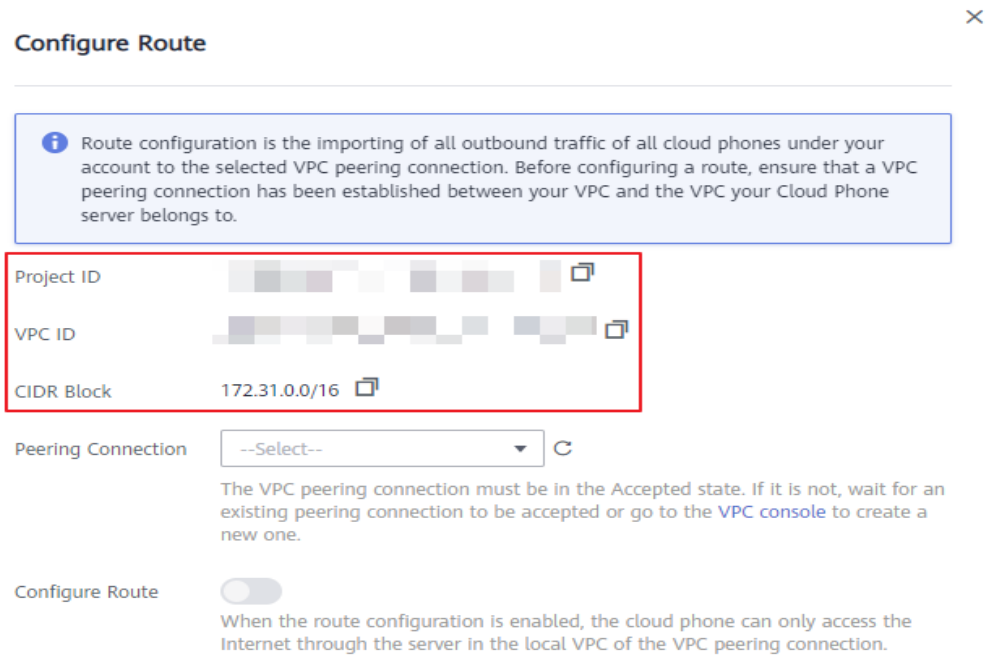
- A Linux ECS is available in your VPC.

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 **Computing** > **Cloud Phone**.

   The Cloud Phone 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.

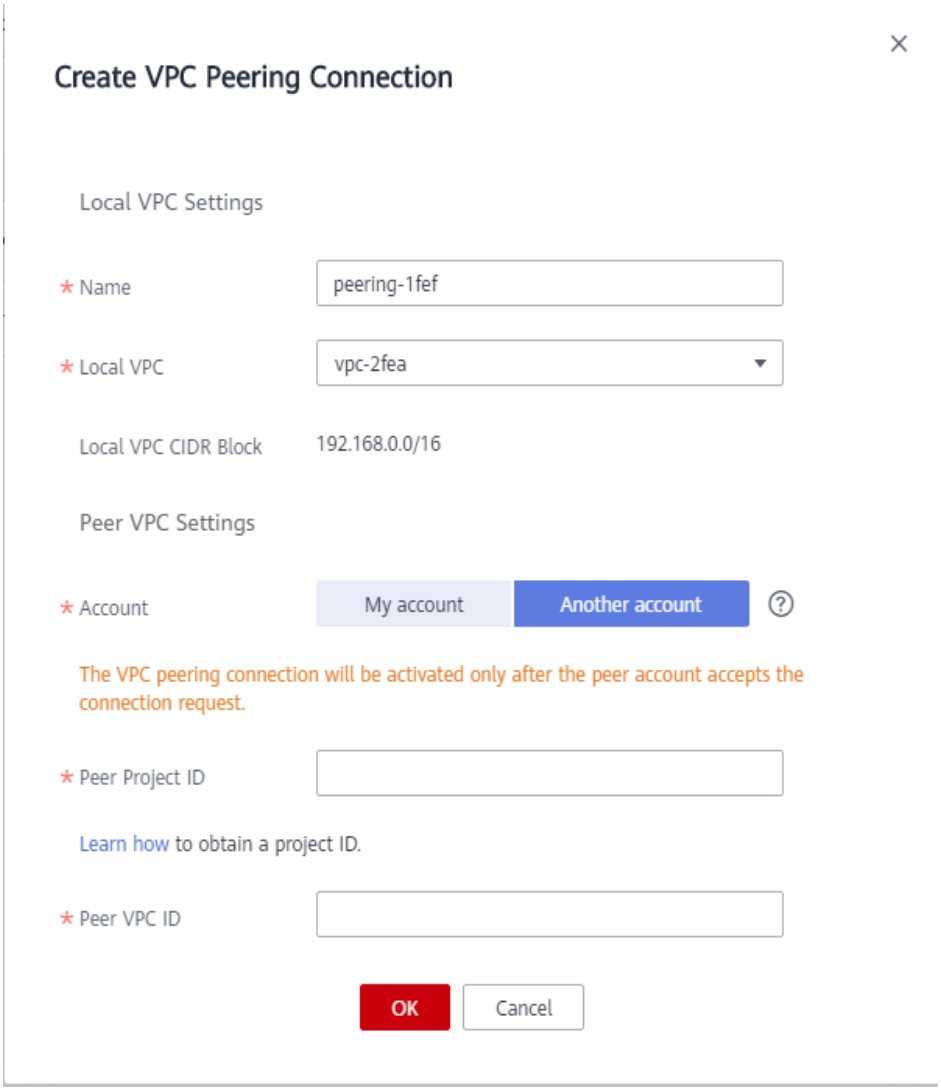
NOTE

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 by referring to **Creating a VPC Peering Connection with a VPC in Another Account**. 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 **Adding Routes for a VPC Peering Connection (Route Table Module Can Be Accessed Through the VPC Details Page)**.

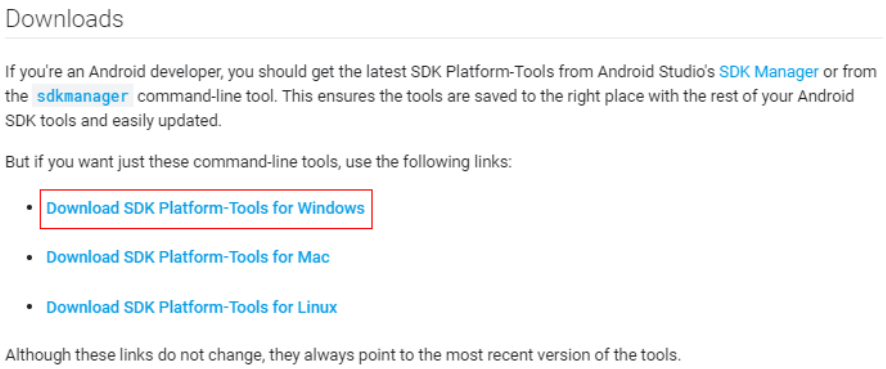
When adding a route, set **Destination** to the CIDR block recorded in **4**. After the route is added, the two VPCs can communicate with each other.

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**.

   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:

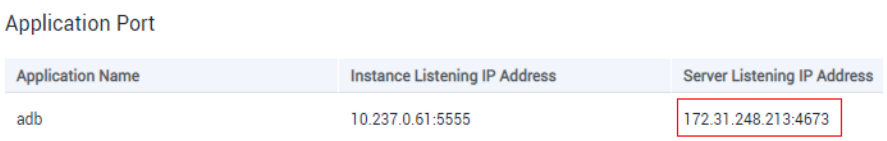
   adb connect *Listening IP address of the server: Listening port number of the server*

   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 2-5 Application Port

   Take the information in **Figure 2-5** as an example. The ADB command is **adb connect 172.31.248.213:4673**.

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 websites:

- **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

- **Displaying the Cloud Phone Screens**
- **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. Therefore, 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 concepts, see **Basic Concepts**.

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

Prerequisites

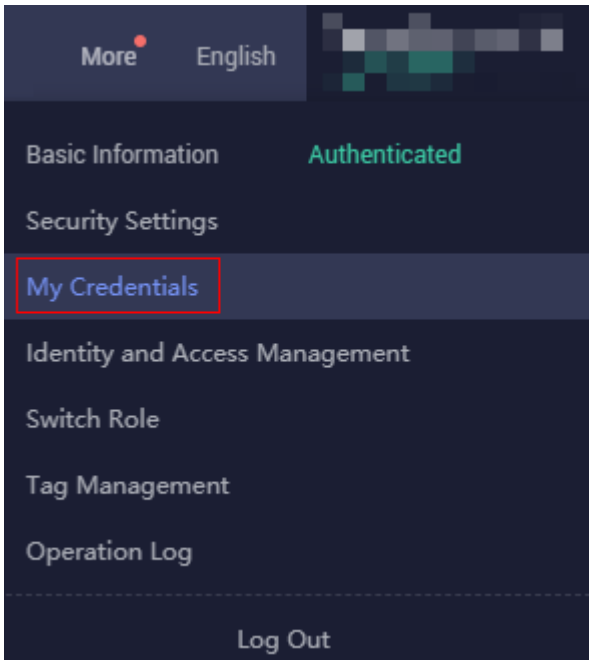
The cloud phone must be in the **Running** state.

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 Cloud Phone console and complete the following preparations:

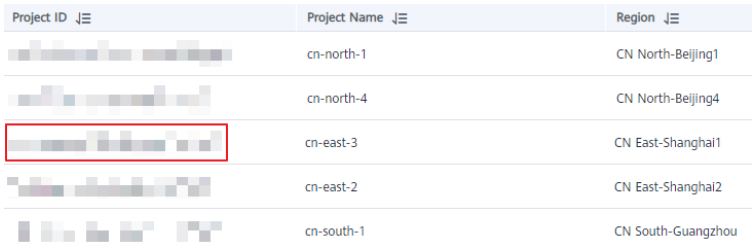
1. Obtain the project ID of the region where the target cloud phone is located. The operations are as follows:

   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.

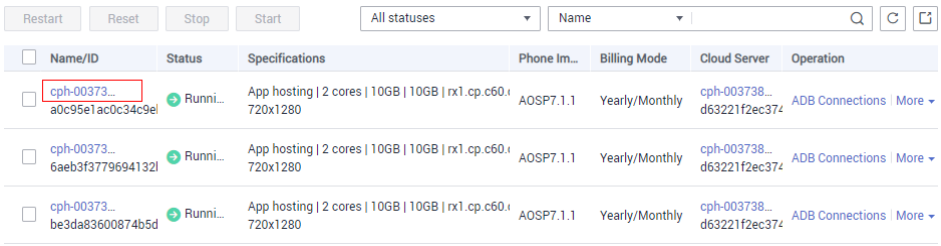
2. Select an idle port on the local device to connect to the cloud phone.

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

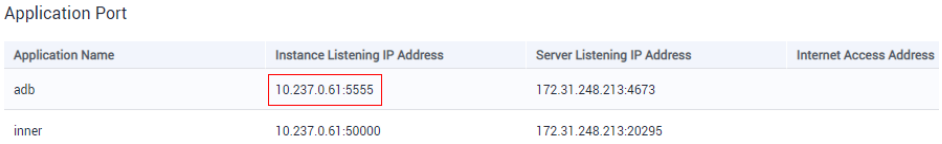
As shown in the following figure, port 6667 is occupied (displayed as **Listening**) by another program, and port 1234 is idle.

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 Cloud Phone 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.

4. Obtain the public IP address of the server. The operations are as follows:

   On the Cloud Phone 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 which the cloud phone belongs to based on the cloud phone name. For example, if the cloud phone name is cph-test-1-00001, the corresponding server name is cph-test-1.

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* **-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, see **2**.
   - *Cloud phone listening IP address*: indicates the private IP address and port number of the cloud phone. For details, see **3**.
   - *SSH tunnel username*: indicates the project ID of the region where the cloud phone is located. For details, see **1**.
   - *Public IP address*: indicates the public IP address of the server. For details, see **4**.
   - *Private key file path*: indicates the local path for storing the private key file corresponding to the server key pair. For details, 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 05e1aexxx, 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 05e1aexxx@xxx.xxx.xxx.xxx -i C:\Users\Administrator\Downloads\KeyPair-a49c.pem -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

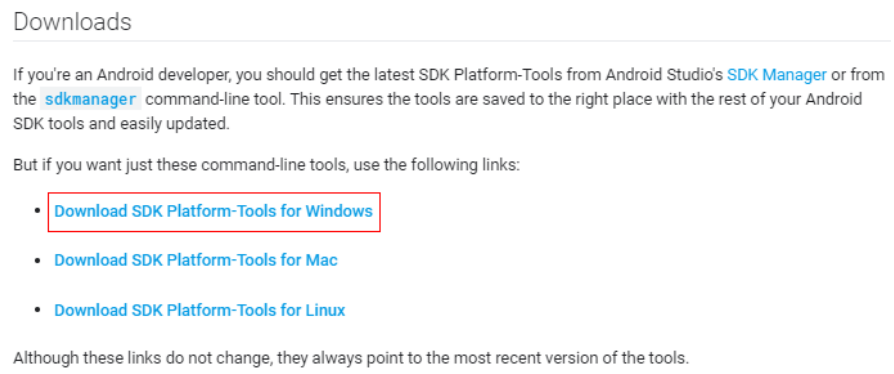
   For details about how to troubleshoot SSH tunnel establishment faults, visit the following websites:

   - **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

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

   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**

   ```
   C:\Users\Administrator\Downloads>adb connect 127.0.0.1:1234
   * daemon not running. starting it now on port 5037 *
   * daemon started successfully *
   ```

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

   ```
   C:\Users\Administrator\Downloads>adb devices
   List of devices attached
   127.0.0.1:1234  device
   ```


NOTE

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

- **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

- **Displaying the Cloud Phone Screens**
- **How Do I Install Applications on a Cloud Phone?**

2.5 VNC (Intranet)

You can use this method to access a cloud phone if the VNC client is not installed on the local device or the remote login to the client fails.

Constraints and Limitations

- When purchasing a Cloud Phone server, you must enable **VNC login** in **Advanced Settings**. If this configuration item is unavailable or disabled, the cloud phone cannot be accessed using VNC.
- Only cloud phones with the rx1.cp.c60.d32.e1v1.qemu flavor support the VNC connection.

Prerequisites

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

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 **Computing** > **Cloud Phone**.

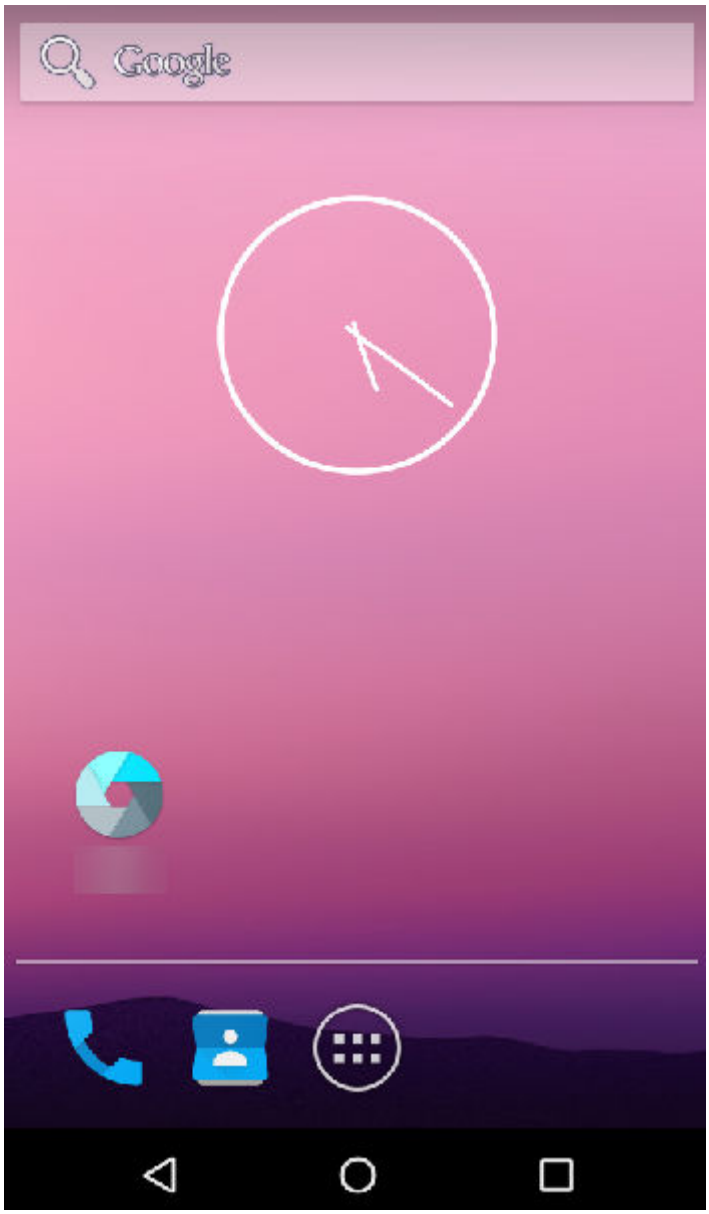
   The Cloud Phone console is displayed.
4. In the navigation pane on the left, choose **Instances**.
5. In the cloud phone list, locate the target cloud phone and click **Log In** in the **Operation** column.

   NOTE

   Only cloud phones with the rx1.cp.c60.d32.e1v1.qemu flavor support remote login.

   Use a mouse to operate the cloud phone.

Figure 2-6 Cloud phone screen



2.6 VNC (Internet)

To access a cloud phone through the Internet, ensure that the VNC client has been installed on the local device. Establish an SSH tunnel first, and then use the VNC client to access the cloud phone.

The local device can run the Windows, Linux, Android, or Mac OS. This topic uses the Windows OS as an example.

Constraints and Limitations

- When purchasing a Cloud Phone server, you must enable **VNC login** in **Advanced Settings**. If this configuration item is unavailable or disabled, the cloud phone cannot be accessed using VNC.

- Only cloud phones with the rx1.cp.c60.d32.e1v1.qemu flavor support the VNC connection.

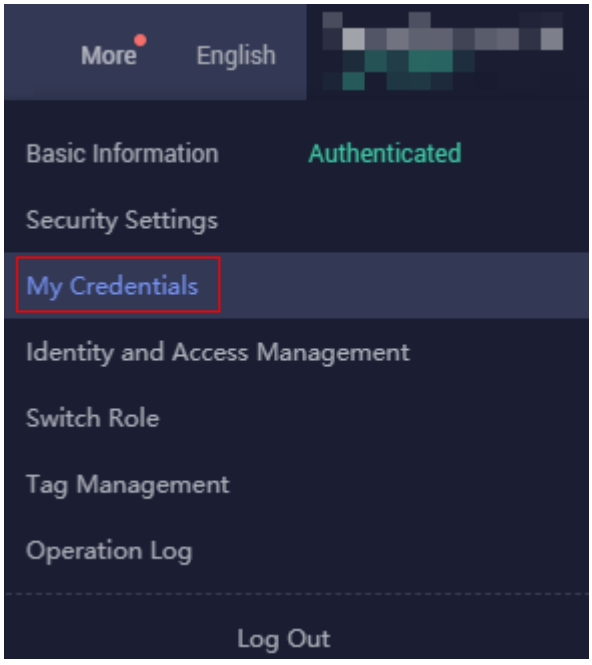
Prerequisites

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

Preparations

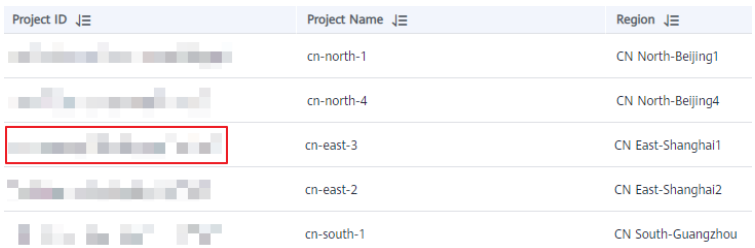
Before establishing an SSH tunnel, ensure that the SSH service has been installed on the local device that will be used to access the cloud phone. For details, see **How Can I Know Whether the SSH Service Has Been Installed on My Local Device?** You also need to log in to the Cloud Phone console and 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.

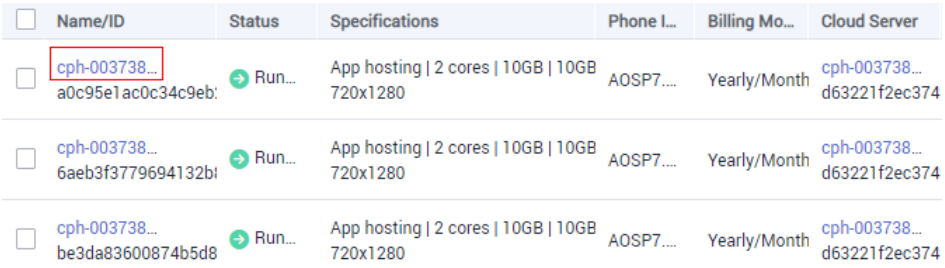
2. Select an idle port on the local device to connect to the cloud phone.

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

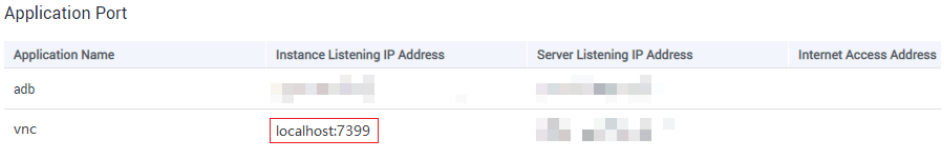
   As shown in the following figure, port 6667 is occupied (displayed as **Listening**) by another program, and port 1234 is idle.

3. Obtain the VNC listening port of the cloud phone. The operations are as follows:

   a. On the Cloud Phone 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 VNC application listening port, for example, 7399 in the following figure.



4. Obtain the public IP address of the server. The operations are as follows:

   On the Cloud Phone 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 which the cloud phone belongs to based on the cloud phone name. For example, if the cloud phone name is cph-test-1-00001, the corresponding server name is cph-test-1.

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:localhost:Cloud phone listening port SSH tunnel username@Public IP address* **-i** *Private key file path* **-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, see 2.
   - *Cloud phone listening port*: indicates the VNC application listening port of the cloud phone. For details, see 3.
   - *SSH tunnel username*: indicates the project ID of the region where the cloud phone is located. For details, see 1.
   - *Public IP address*: indicates the public IP address of the server. For details, see 4.
   - *Private key file path*: indicates the local path for storing the private key file corresponding to the server key pair. For details, see 5.

   Assume that the local idle port is 1234, the listening port of the cloud phone is 7399, the SSH tunnel username is 05e1aexxx, 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:localhost:7399 05e1aexxx@xxx.xxx.xxx.xxx -i C:\Users\Administrator\Downloads\KeyPair-a49c.pem -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 7399 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

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

- **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 Use the VNC Client to Access the Cloud Phone

Use the VNC client, such as VNC Viewer, to access the cloud phone.

NOTE

To download VNC Viewer, log in at **https://www.realvnc.com/en/connect/download/viewer/**.

Enter the IP address and port number based on the VNC client usage, for example, 127.0.0.1: Local idle port.

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

3 Cloud Phone Management

3.1 Querying Details of a Cloud Phone

This section describes how to query details of a cloud phone on the Cloud Phone 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 **Computing** > **Cloud Phone**.

   The Cloud Phone 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, and Phone Image ID

     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

     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.

3.2 Restarting Cloud Phones

This topic describes how to restart a cloud phone or multiple cloud phones on the Cloud Phone 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 Cloud Phone console or by calling the Cloud Phone API. For details, see **Restarting Cloud Phones**.

Prerequisites

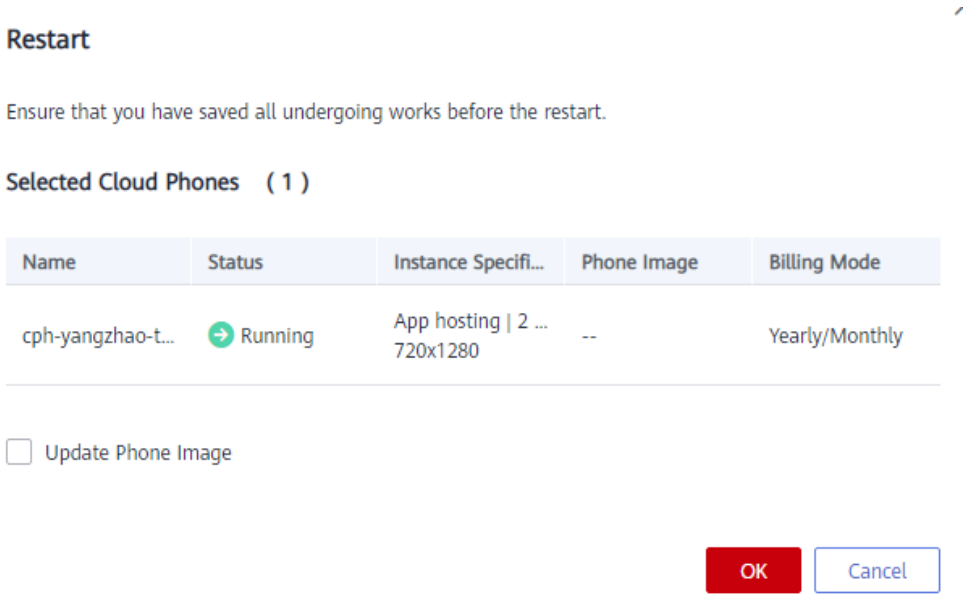
- Before the restart, ensure that all files on the cloud phone have been saved to prevent file loss.
- The cloud phone must be in the **Running** or **Stopped** state. If the cloud phone is in other states, such as **Faulty**, **Stopping**, and **Creating**, it cannot be restarted.

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 **Computing** > **Cloud Phone**.

   The Cloud Phone 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 3-2 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.

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

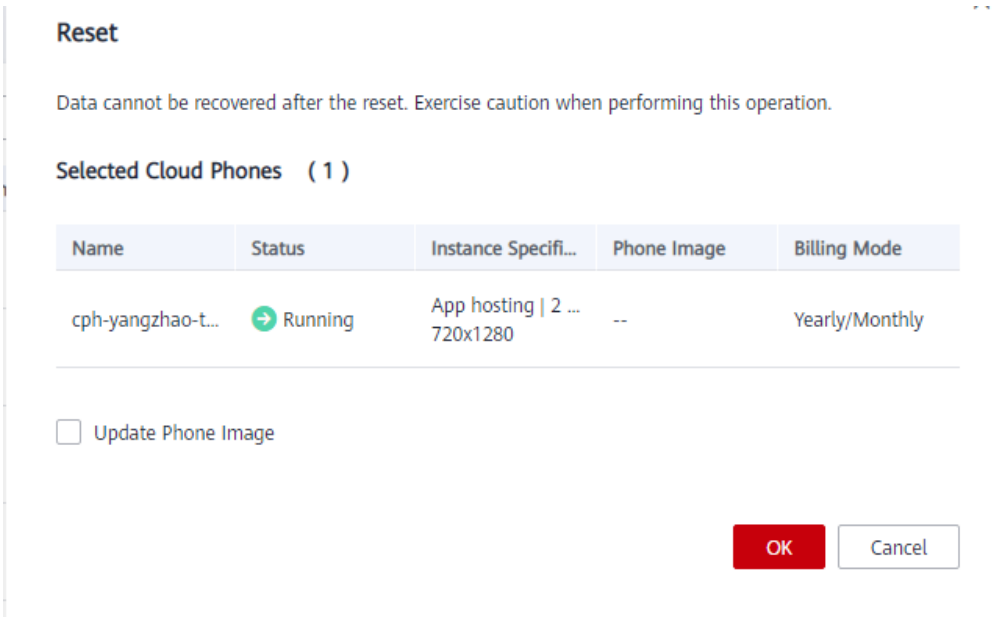
The cloud phone cannot be restored after being reset. Exercise caution when performing this operation.

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 **Computing** > **Cloud Phone**.

   The Cloud Phone 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 3-3 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.

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 Cloud Phone console.

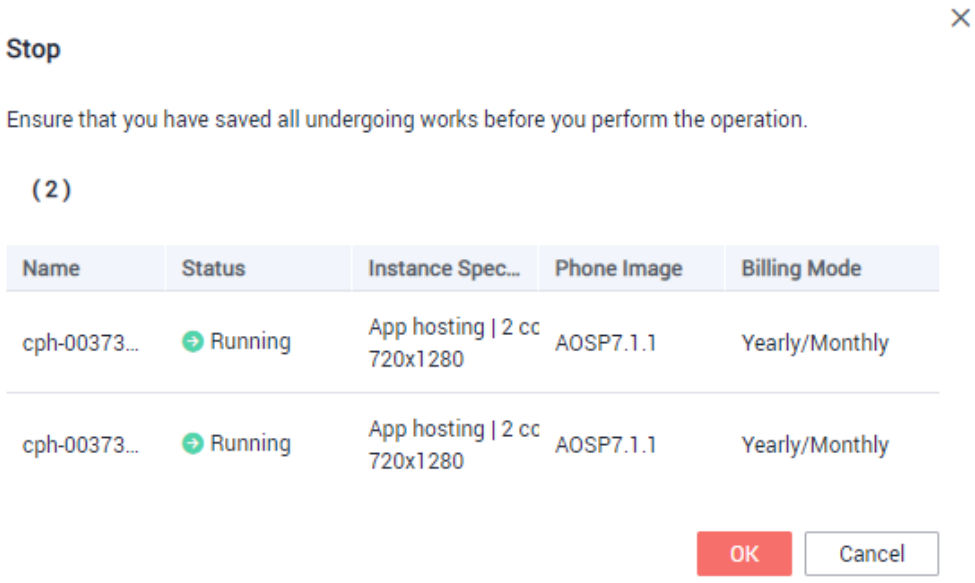
Prerequisites

- 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 **Computing** > **Cloud Phone**.
   The Cloud Phone 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 3-4 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 Cloud Phone console.

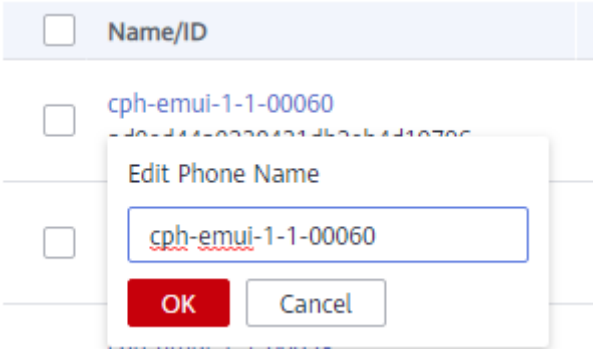
Procedure

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 **Computing** > **Cloud Phone**.

   The Cloud Phone 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 3-5 Edit Phone Name

6. Click **OK**.

   The new name will take effect.

Associated APIs

Editing the Name of a Cloud Phone

3.6 Updating Cloud Phone Attributes

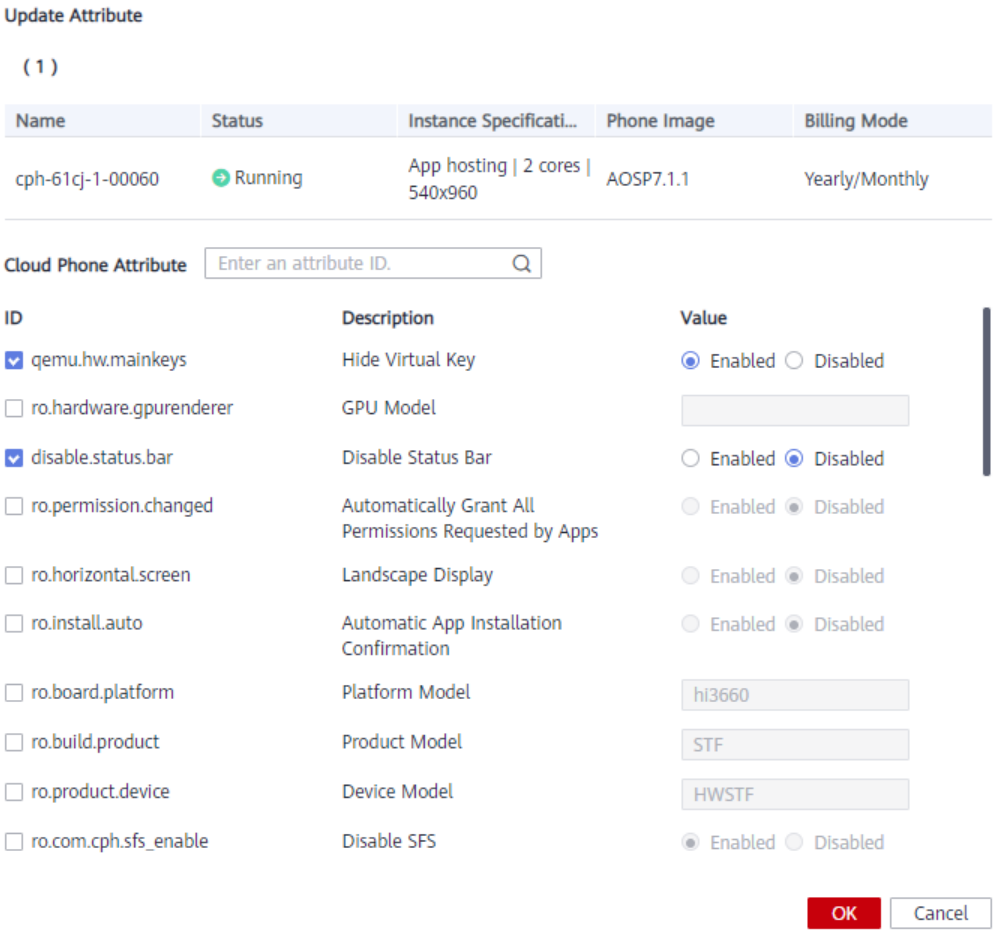
This section describes how to update the cloud phone attributes on the console, such as the product model, device model, whether to hide the virtual key, and whether to display the cloud phone in landscape mode.

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 **Computing** > **Cloud Phone**.

   The Cloud Phone 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 3-6 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 Cloud Phone built-in account, and install and update the APK by file push. For details, see **Pushing Files**.

Constraints and Limitations

Cloud Phone 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.
- If you need 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.
- If you need 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 server, the time consumed by file push is directly proportional to the number of files pushed.

Procedure

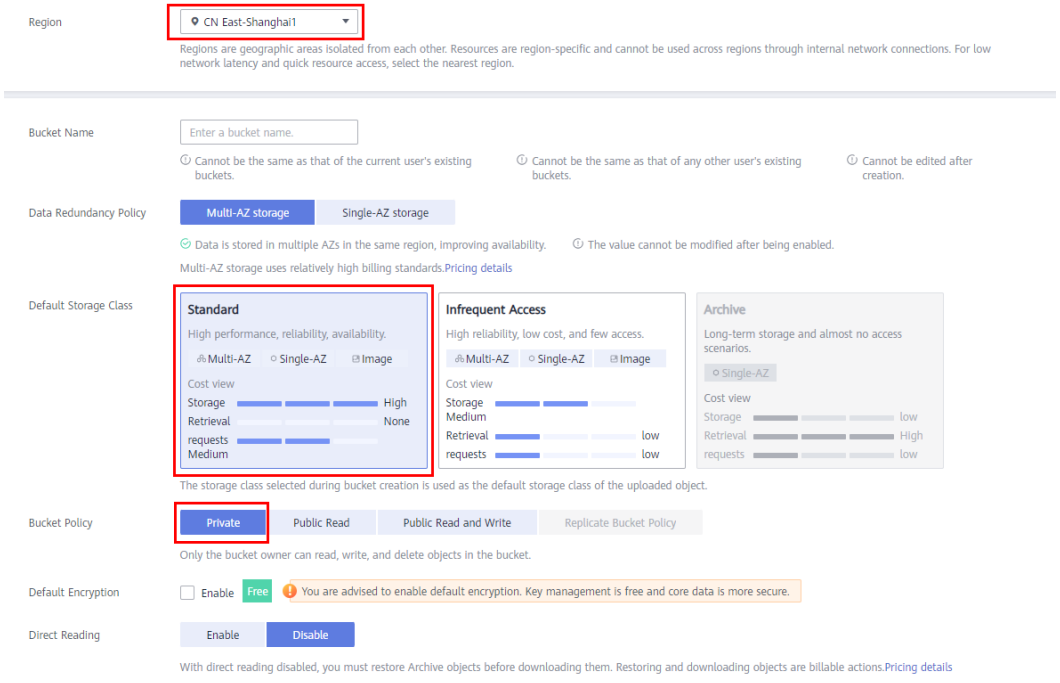
The following procedure demonstrates how to create a bucket for storing files and how to set permissions for the bucket. You can install and update APK only by invoking APIs.

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 3-7 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**.

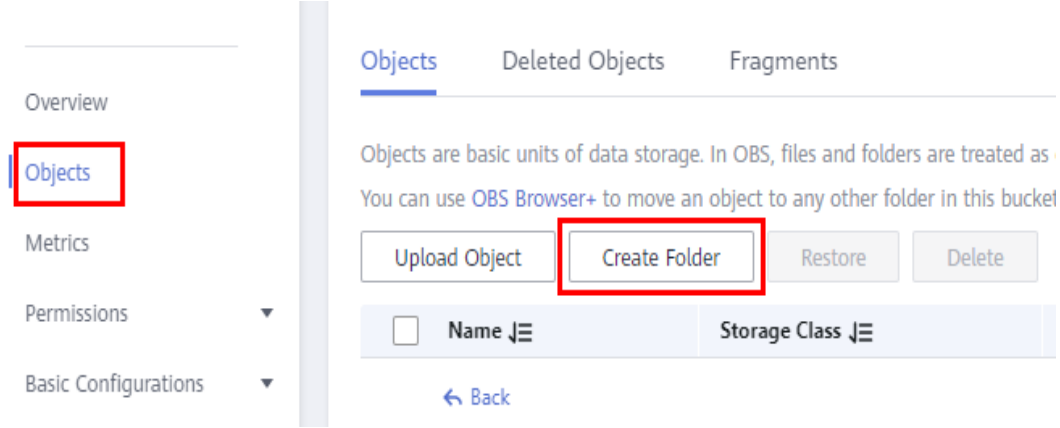
For details about other parameters, see **Creating a Bucket**.

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**.

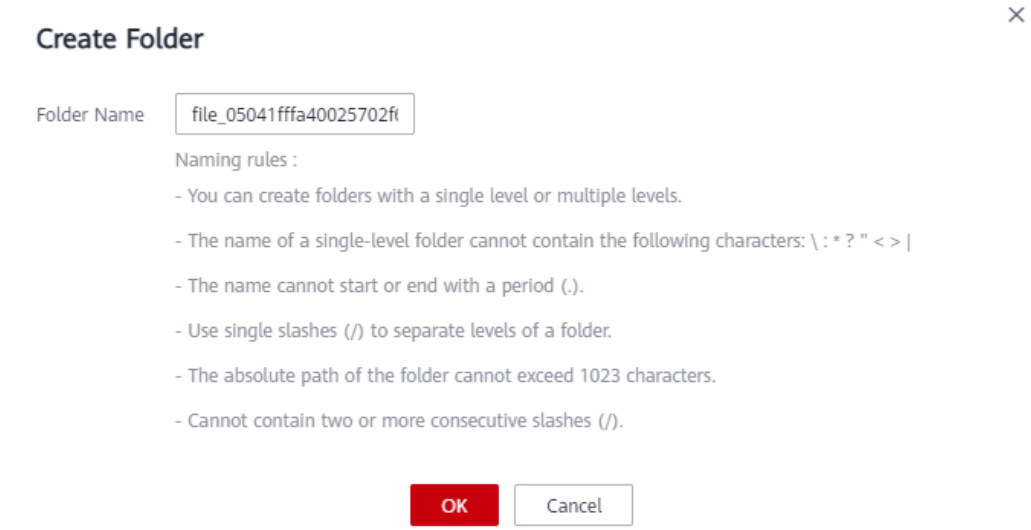
Figure 3-8 Objects



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

   {project_id} is the project ID of 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 3-9 Creating the **file_{project_id}_01** folder

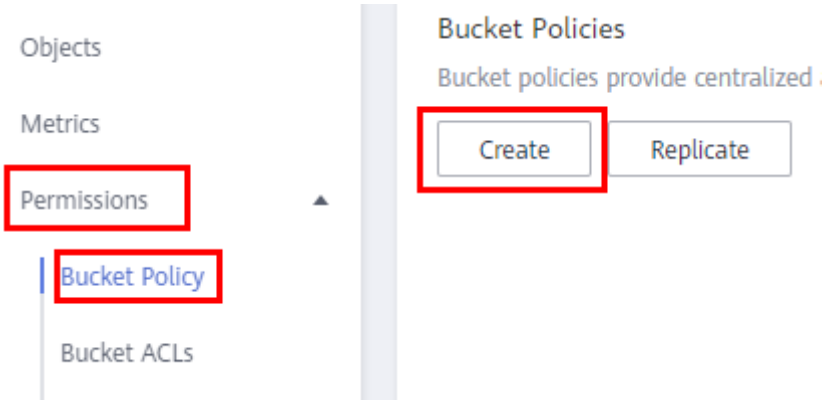


   NOTE

   - 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 facilitate 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.

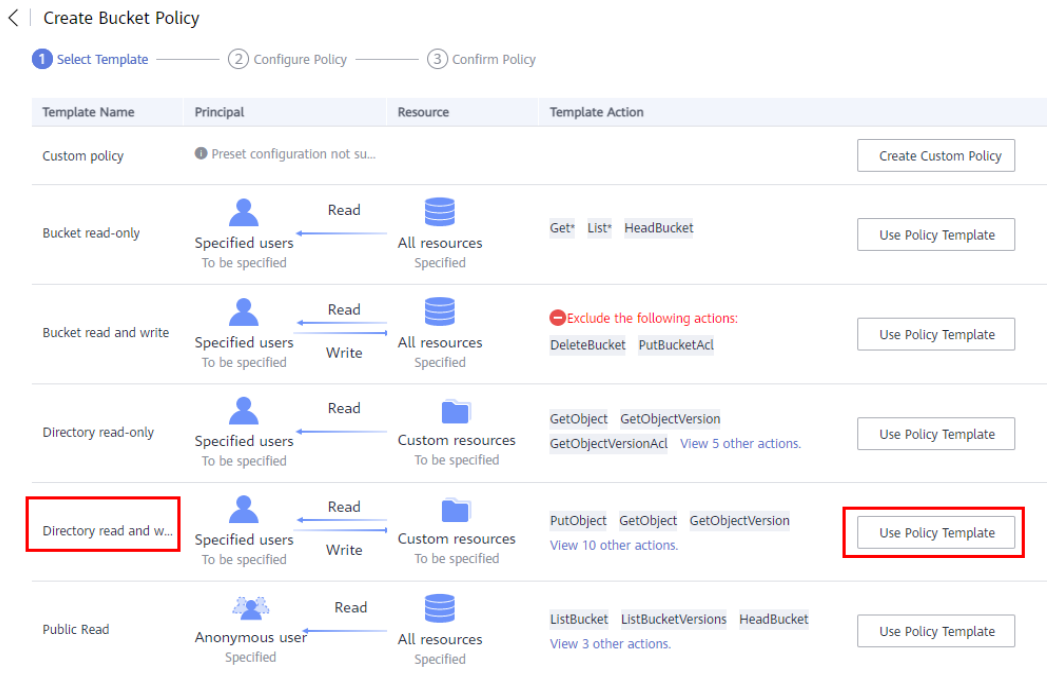
7. In the navigation pane on the left, choose **Permissions** > **Bucket Policy**. On the displayed page, click **Create**.

   Figure 3-10 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 Cloud Phone built-in account. Click **Use Policy Template**.

Figure 3-11 Select Template



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

     CAUTION

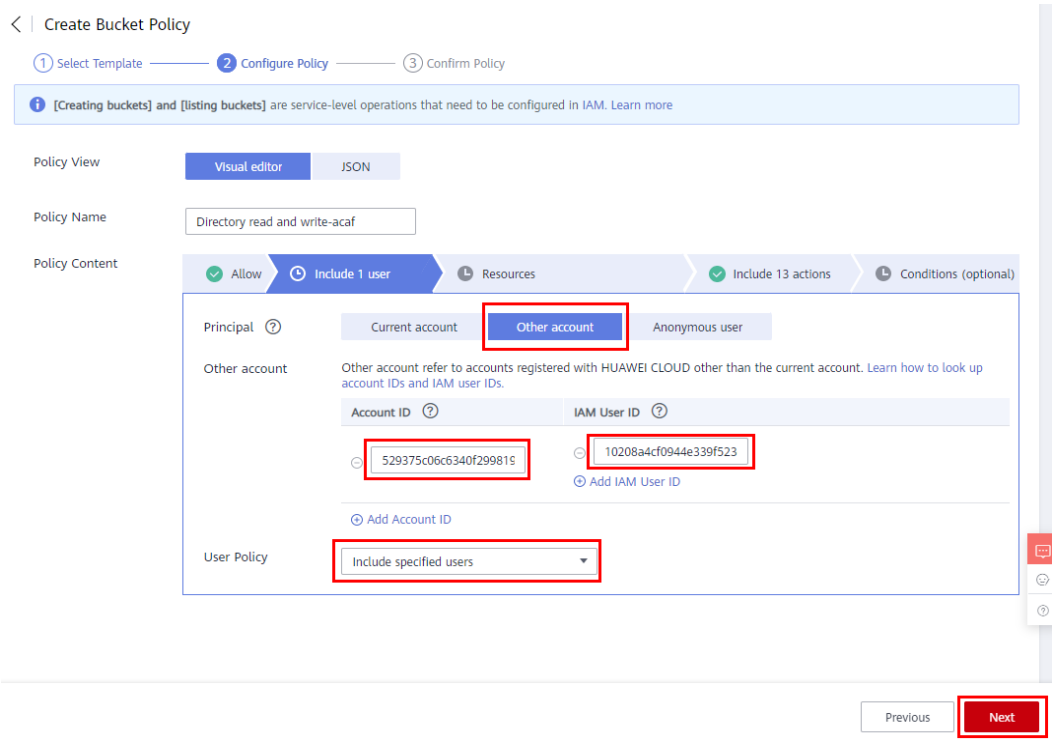
     The Cloud Phone built-in account is mandatory and must contain the following information. You cannot enter the ID of your own account.

     Account ID: **529375c06c6340f299819082b3051225**

     IAM User ID: **10208a4cf0944e339f523d9943ba02d3**

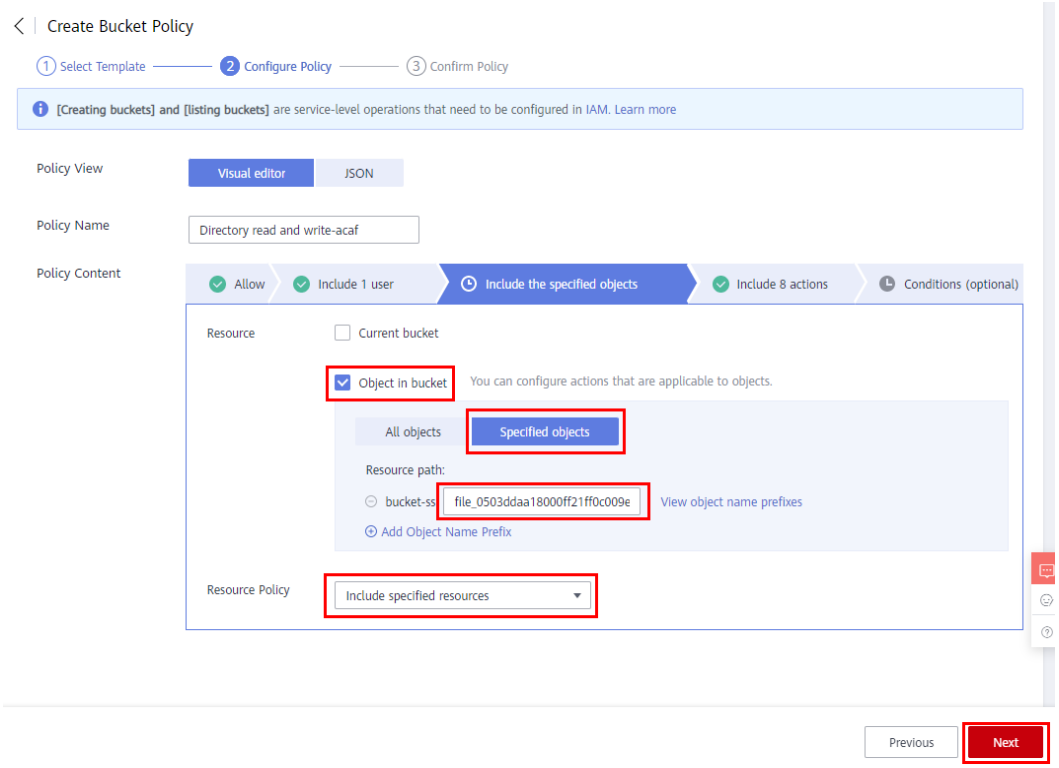
   - **User Policy**: Select **Include specified users**.

Figure 3-12 Configure Policy



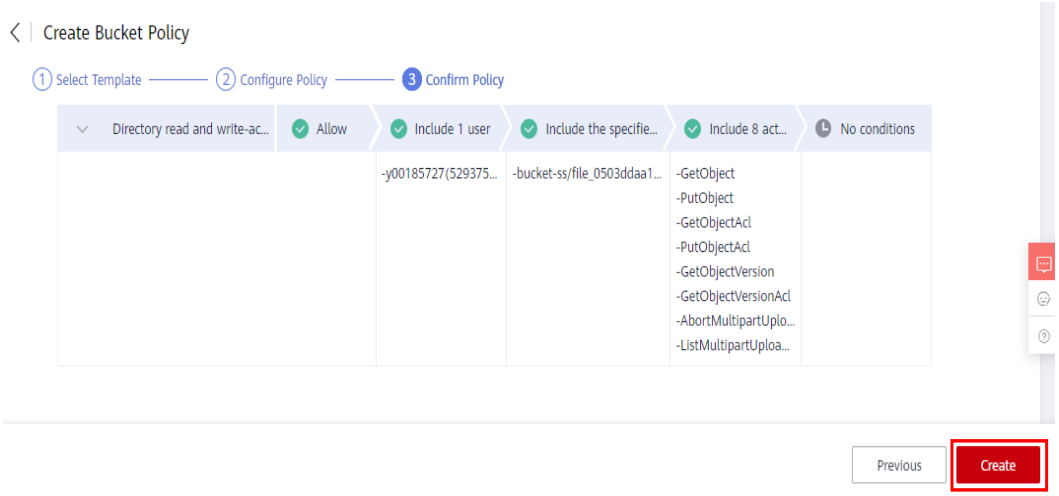
10. For resource, select **Specified object** in the current bucket and enter the resource name **file_{project_id}_***, for example, **file_0503ddaa18000ff21ff0c009e65d5482_***. Select **Include specified resources** for **Resource Strategy** and click **Next**.

Figure 3-13 Specified objects



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

Figure 3-14 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 Server Management

4.1 Editing a Server Name

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

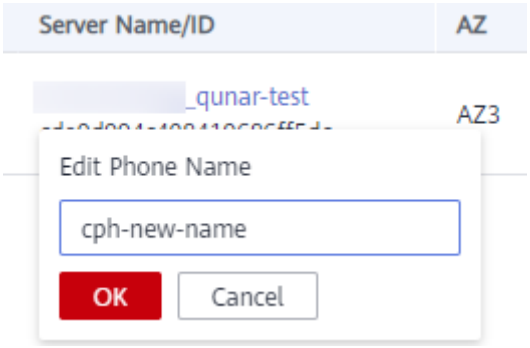
Procedure

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 **Computing** > **Cloud Phone**.

   The Cloud Phone 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 a Server

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

Prerequisites

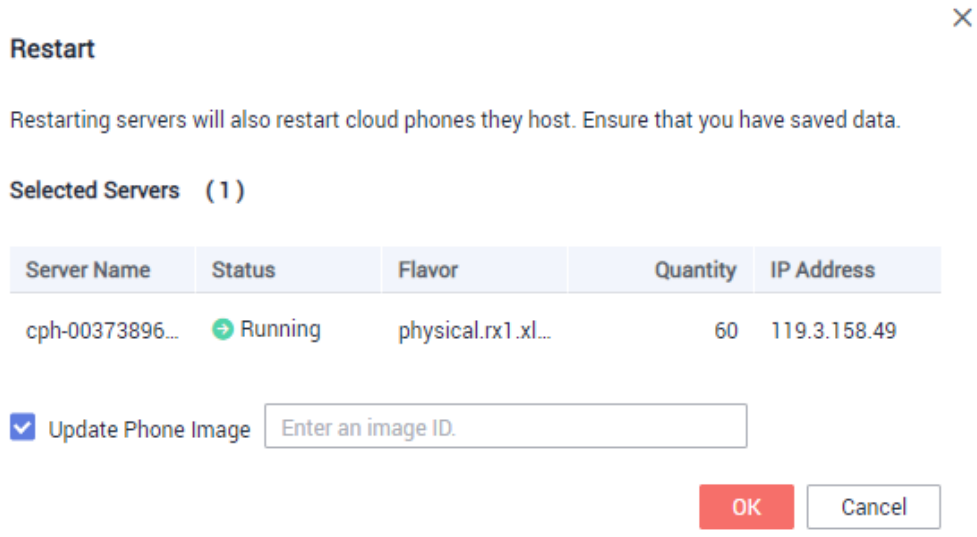
Restarting the server will disconnect the cloud phone. Save data before the restart.

Procedure

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

   The Cloud Phone 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**.

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 target server is located.
3. On the **Service List** page, choose **Computing** > **Cloud Phone**.

   The Cloud Phone 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 target server is located.
3. On the **Service List** page, choose **Computing** > **Cloud Phone**.

   The Cloud Phone 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.

5 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.

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 you want to access the Internet, you can only use a server in the VPC corresponding to the VPC peering connection you have selected.

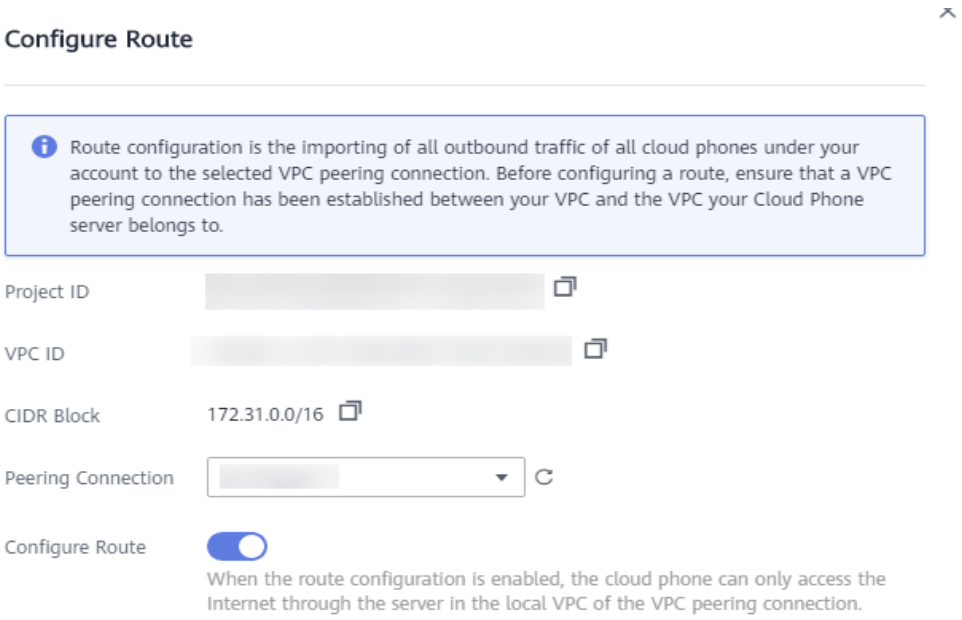
Prerequisites

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 **Computing** > **Cloud Phone**.
   The Cloud Phone 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 5-1 Configure Route



Execution Result

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

6 Permission Management

6.1 Creating a User and Granting Cloud Phone Permissions

This section describes how to use **IAM** to implement fine-grained permissions control for your Cloud Phone 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 Cloud Phone resources.

If your HUAWEI CLOUD account does not need individual IAM users, skip this chapter.

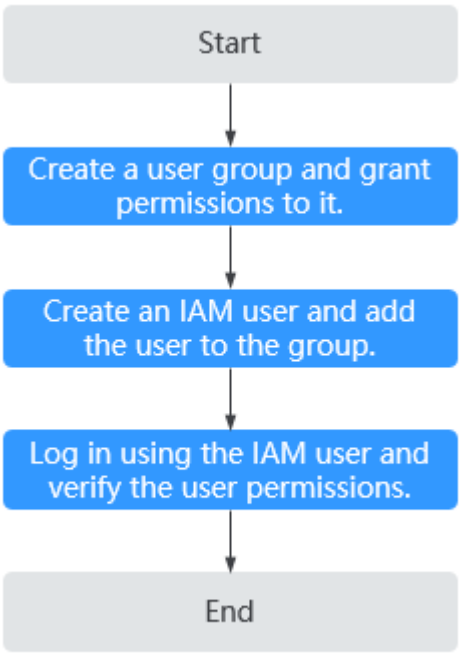
This section uses the **CPH User** policy as an example to describe how to grant permissions to a user. **Figure 6-1** shows the process.

Prerequisites

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

Authorization Process

Figure 6-1 Process for granting Cloud Phone 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.**

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

3. **Log in Using an IAM User** 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**. Under **Computing**, select **Cloud Phone**. 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**. Under **Computing**, select **Cloud Phone**. On the displayed Cloud Phone console, check whether the **Buy Server** button is displayed in the upper right corner. If no, the read-only permission has taken effect.

7 Adjusting Resource Quotas

What Is a Quota?

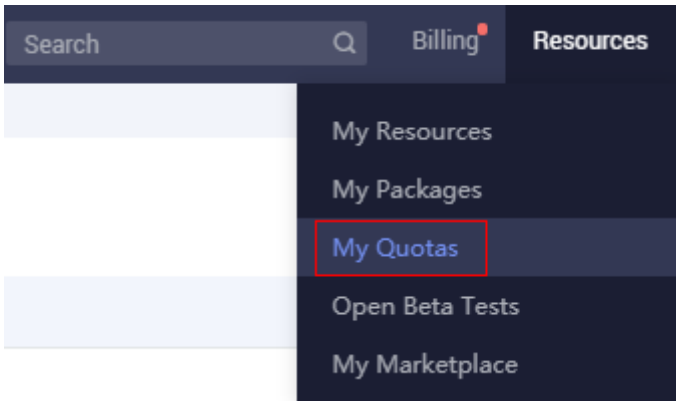
Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number and capacity of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

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. In the upper left corner, select the target region.
3. In the upper right corner of the page, choose **Resources** > **My Quotas**.
   The **Service Quota** page is displayed.

   Figure 7-1 My Quotas



4. View the total and used quota of service resources on the displayed page.

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.

3. In the upper right corner, click **Increase Quota**.
4. On the **Create Service Ticket** page, configure parameters as required.

   In **Problem Description** area, fill in the content and reason for adjustment.
5. Select **I have read and agree to the Tenant Authorization Letter**, and click **Submit**.

   After the quota is successfully adjusted, a message will be sent to you immediately.

8 Monitoring

8.1 Supported Metrics

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

Namespace

SYS.CPH

Metrics

Cloud Phone supports the following metrics: Cloud Phone server metrics (**Table 8-1**), cloud phone metrics (**Table 8-2**), disk metrics (**Table 8-3**), and GPU metrics (**Table 8-4**).

Table 8-1 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
downstream_bandwidth	Inbound Bandwidth	Network rate (inbound)	≥ 0 bits/s	Cloud Phone server	1 minute
upstream_bandwidth	Outbound Bandwidth	Network rate (outbound)	≥ 0 bits/s	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
upstream_bandwidth_usage	Bandwidth Usage (Outbound)	Bandwidth usage (outbound)	0-100%	Cloud Phone server	1 minute
up_stream	Outbound Traffic	Network traffic going out from the cloud platform (previously called Upstream Traffic)	≥ 0 bytes/s	Cloud Phone server	1 minute
down_stream	Inbound Traffic	Network traffic coming into the cloud platform (previously called Downstream Traffic)	≥ 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 8-2 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 usage (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
cph_disk_agt_read_bytes_rate	I/O Read Rate	Bytes/second read from the block device of the cloud phone	≥ 0 bytes/s	Cloud phone	1 minute
cph_disk_agt_write_bytes_rate	I/O Write Rate	Bytes/second written to the block device of the cloud phone	≥ 0 bytes/s	Cloud phone	1 minute
cph_disk_usedPercent	Disk Usage	Cloud phone disk usage	0-100%	Cloud phone	1 minute

Table 8-3 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 8-4 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

Dimensions

Key	Value
instance_id	Cloud Phone server IDs
cph_id	Cloud phone IDs
disk_name	Disk names
gpu_index	GPU names

8.2 Viewing Cloud Phone 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. Under **Management & Deployment**, select **Cloud Eye**.
4. In the navigation pane on the left, choose **Cloud Service Monitoring** > **Cloud Phone**.
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.

8.3 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**.
   - **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.

9 CTS

9.1 Key Cloud Phone Operations Recorded by CTS

Cloud Trace Service (CTS) is a log audit service intended for Huwei 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 Cloud Phone 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 9-1 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

9.2 Viewing Tracing Logs

After CTS is enabled, it starts recording operations on your cloud phones. You can view operation records of the last seven days on the CTS management console.

This topic describes how to view the operation records.

Procedure

1. Log in to the management console.
2. In the upper left corner, select the target region.
3. Click **Service List**. Under **Management & Deployment**, select **Cloud Trace Service**.
4. In the navigation pane on the left, choose **Trace List**.
5. Specify filter criteria and click **Query**.

   The following four filter criteria are available:

   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**

     Select a filter criterion from the drop-down list. Set **Trace Type** to **Management**, **Trace Source** to **CPH**, and **Resource Type** to **phone**.

     Figure 9-1 Setting filter criteria

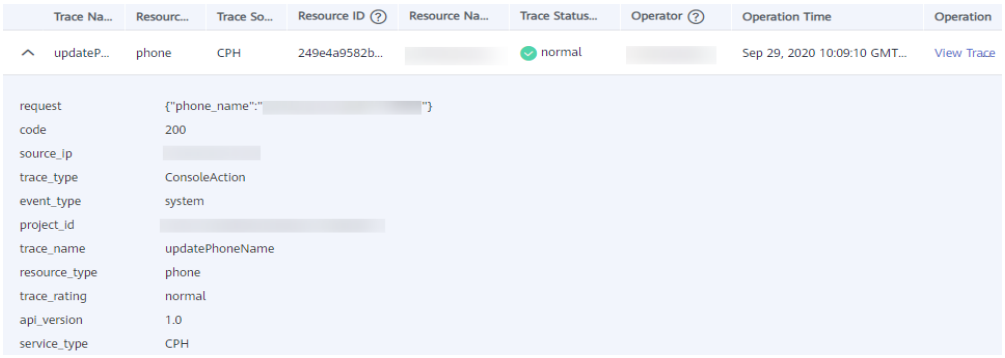
     Where,

     - If you select **Resource ID** for **Search By**, enter a specific resource ID. Only whole strings are matched.
     - If you select **Resource name** for **Search By**, select or enter a specific resource name.

   - **Operator**: Select a specific operator from the drop-down list.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: You can select **Last 1 hour**, **Last 1 day**, **Last 1 week**, and **Customize**.

6. Click ⌄ on the left of a trace to expand its details.

Figure 9-2 Expanding a trace



7. Locate the row containing the target trace and click **View Trace** in the **Operation** column.

Figure 9-3 View Trace

For details about key fields in the CTS trace structure, see **Trace Structure**.

A Change History

Released On	Description
2021-09-30	This issue is the eleventh official release, which incorporates the following change: Added Device Emulation and Cloud Phone Audio and Video.
2021-05-11	This issue is the tenth official release, which incorporates the following change: Added **#li85755276437**.
2021-02-25	This issue is the ninth official release, which incorporates the following change: Added Using AOSP.
2021-02-10	This issue is the eighth official release, which incorporates the following change: Added the description of custom network configuration in **Buying a Cloud Phone (with Detailed Parameter Description)**.
2020-09-30	This issue is the seventh official release, which incorporates the following changes: • Added **CTS**. • Updated the screenshots for network configuration in **Buying a Cloud Phone (with Detailed Parameter Description)**.

Released On	Description
2020-08-10	This issue is the sixth official release, which incorporates the following changes: • Added **User-defined Network** in **Buying a Cloud Phone (with Detailed Parameter Description)**. • Modified the method of creating a VPC peering connection in **ADB (Intranet)**. • Added sections Exporting Cloud Phones, **Configuring a Route**, and **Monitoring**.
2020-06-22	This issue is the fifth official release, which incorporates the following change: Added **Updating Cloud Phone Attributes**.
2020-04-30	This issue is the fourth official release, which added the following sections: • **Querying Details of a Cloud Phone** • **Stopping Cloud Phones** • **Editing the Name of a Cloud Phone** • **Restarting a Server** • **Unsubscribing from a Server** • **Renewing a Server**
2020-03-30	This issue is the third official release, which incorporates the following change: Added **ADB (Recommended)**.
2020-02-18	This issue is the second official release, which incorporates the following change: Optimized the whole document, including adjusting the outline, optimizing procedure descriptions, and adding scenario descriptions.
2019-01-31	This issue is the first official release.