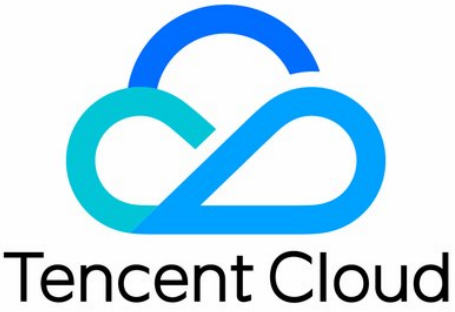
Intelligent Viewdata Computing Practical Tutorial



Copyright Notice

Trademark Notice

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Practical Tutorial
GB/T28181 Protocol Access Practice

Last updated: 2024-08-15 09:51:57

This document introduces how to access devices through the GB28181 protocol to IVC.

> **Note:**
> You can also watch GB/T28181 Protocol Access Demonstration Video to understand the overall access process.

Access Configuration Process

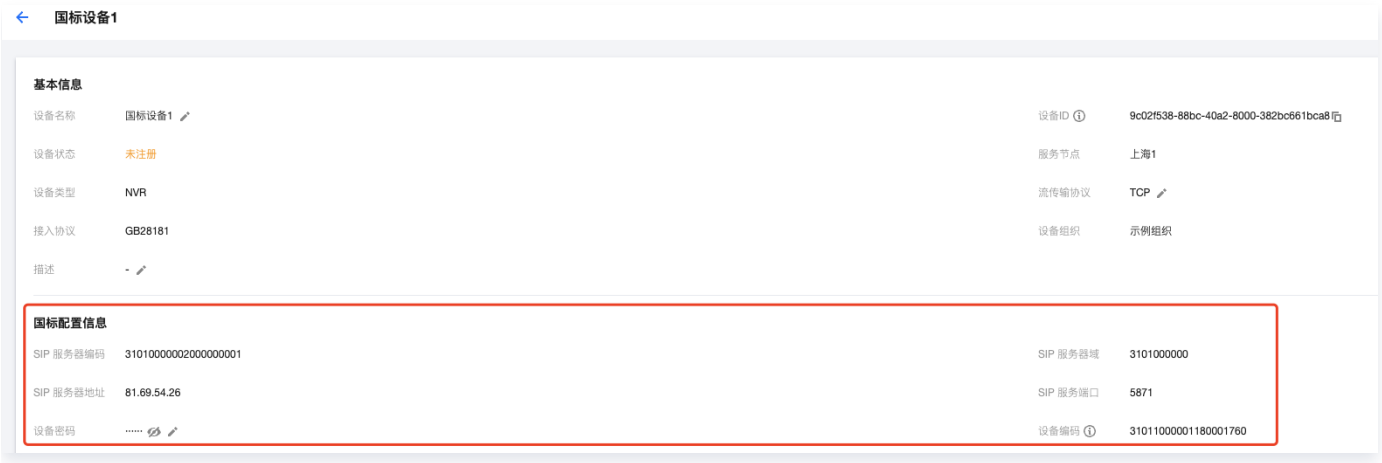
Step 1: Create devices in the console

1. log in to IVC Console.
2. In the left navigation bar, select the **Device Access** feature, and first navigate to Device Organization **Device Organization**. Select the corresponding device organization, click **Add Device** (you can choose **Manual Addition or Bulk Import**. This document explains manual addition as an example).

3. After the device is successfully created, its initial status is **Unregistered**.

Step 2: Obtain device national standard configuration information

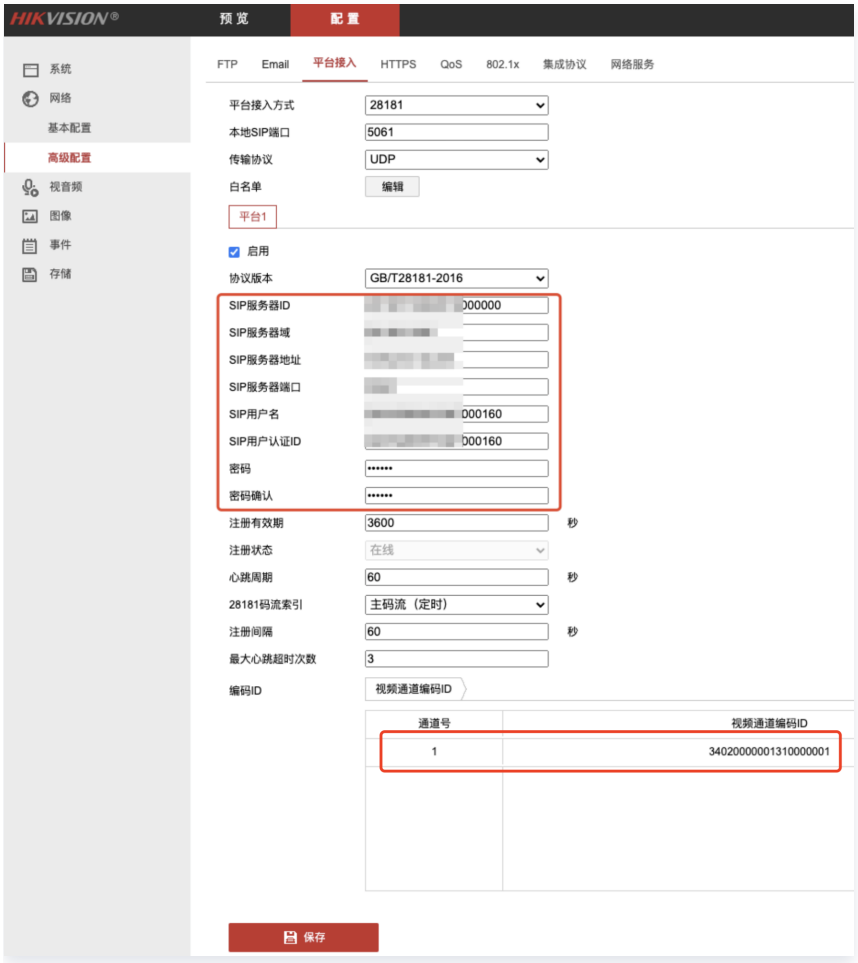
click the device name to enter the **Device Details** page, and view and record the configuration information generated for the device (as shown in the red box below).



> **Note:**
> When there are many devices, it is recommended to use the **Export Device Information** feature to export device configuration information in bulk.

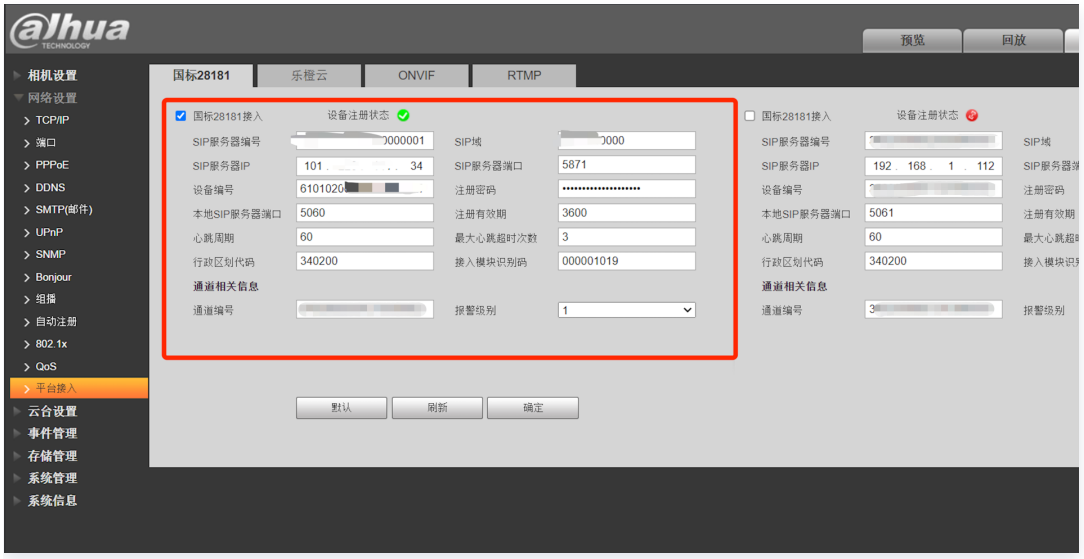
Step 3: log in to the device Web interface for configuration

Hikvision device configuration example (using IPC as an example)



Configuration Parameters	Configuration Instructions
Local SIP Port	**Must be changed to other port numbers like 5061, 5062, etc.** (Do not use the device's default port number 5060, as it may be blocked by the router).
Transfer protocol	This refers to the protocol used for signaling transmission, **prioritize choosing the TCP protocol.**
Protocol Version	Select GB/T28181–2016.
SIP Server ID	Enter the SIP Server ID generated by the platform in Step 2.
SIP Server Domain	Enter the SIP Server Domain generated by the platform in Step 2**(it's the first 10 digits of the SIP Server ID)**.
SIP Server Address	Enter the SIP Server IP generated by the platform in Step 2.
SIP Server Port	Enter the SIP Server Port number generated by the platform in Step 2.
SIP Username and SIP User Authentication ID	Enter the device code generated by the platform in Step 2, for example: 34020000001320000001
Password and Password Confirmation	Enter the device password in Step 2 **(entered when creating the device in the console)**.
Registration Validity Period	The validity period for the device registration on the platform.**It is recommended to use the default value of 3600s**.
Heartbeat Interval	The time interval at which the device sends heartbeat information.**It is recommended to use the default value of 60s**.
Maximum Timeout Count	If the heartbeat continuously times out and reaches the "maximum number of timeouts," the device is considered unable to establish a connection with the platform.**It is recommended to use the default value of 3 times**.
Video Channel Encoding ID	The rule is consistent with the SIP username. Change the 11th–13th digits to 131, and it is recommended to write them in ascending order based on the channel number, ensuring no duplicates, for example: 34020000001310000001, 34020000001310000002, **Note:** • **Just ensure that the channel coding ID here does not repeat with the above [SIP username], otherwise, it will prompt "parameter error". However, it doesn't matter if it's the same as the channel coding ID of other devices.** • **The same rule applies when configuring NVR devices here.**

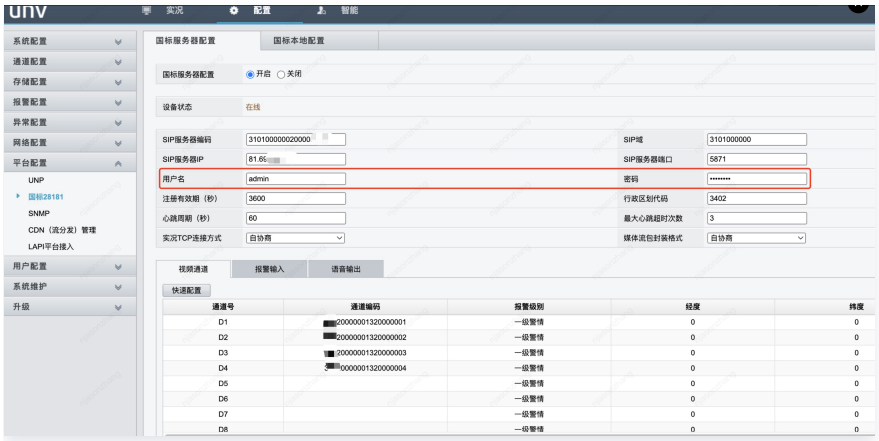
Dahua Device Configuration Example (using IPC as an example)



Parameter Configuration	Configuration Instructions
SIP Server Number	Enter the SIP Server ID generated by the platform in Step 2.
SIP Server Domain	Enter the SIP Server Domain generated by the platform in Step 2 (the first 10 digits of the SIP Server ID).
SIP Server IP	Enter the SIP Server IP generated by the platform in Step 2.
SIP Server Port	Enter the SIP Server Port number generated by the platform in Step 2.
Device Number	Enter the device code generated by the platform in Step 2, for example: 34020000001320000001
Registration Password	Enter the device password in Step 2 (entered when creating the device in the console).
Local SIP Server Port	**Must be changed to other port numbers like 5061, 5062, etc.** (Do not use the device's default port number 5060, as it may be blocked by the router).
Registration Validity Period	The validity period for the device registration on the platform. It is recommended to use the default value of 3600s.
Heartbeat Interval	The time interval at which the device sends heartbeat information. It is recommended to use the default value of 60s.
Maximum Timeout Count	If the heartbeat continuously times out and reaches the "maximum number of timeouts," the device is considered unable to establish a connection with the platform. It is recommended to use the default value of 3 times.

Channel Number	The rule is consistent with the SIP username. Change the 11th–13th digits to 131, and it is recommended to set them in ascending order based on the channel number, ensuring no duplicates, for example: 34020000001310000001, 34020000001310000002, **Note:** • **Just ensure that the channel encoding ID here does not repeat with the above [Device Number], otherwise, it will prompt "parameter error." However, it doesn't matter if it's the same as the channel encoding ID of other devices.** • **The same rule applies when configuring NVR devices here.**

Yushi Device Configuration Demonstration (using NVR as an example)



Parameter Configuration	Configuration Instructions
SIP Server Code	Enter the SIP Server ID generated by the platform in Step 2.
SIP Domain	Enter the SIP Server Domain generated by the platform in Step 2 (the first 10 digits of the SIP Server ID).
SIP Server IP	Enter the SIP Server IP generated by the platform in Step 2.

SIP Server Port	Enter the SIP Server Port number generated by the platform in Step 2.
Username	Log in to the device Web end with the username. **Note:** Do not enter the device code generated by the platform here.
Password	Enter the device password in Step 2 (entered when creating the device in the console).
Registration Validity Period	The validity period for the device registration on the platform. It is recommended to use the default value of 3600s.
Heartbeat Interval	The time interval at which the device sends heartbeat information. It is recommended to use the default value of 60s.
Maximum Timeout Count	If the heartbeat continuously times out and reaches the "maximum number of timeouts," the device is considered unable to establish a connection with the platform. It is recommended to use the default value of 3 times.
Channel Number	The rule is consistent with the SIP username. Change the 11th–13th digits to 131, and it is recommended to set them in ascending order based on the channel number, ensuring no duplicates, for example: 34020000001310000001, 34020000001310000002,
Local GB Configuration	**Enter the device code generated by the platform in Step 2,** for example: 34020000001320000001

Step 4: Complete the configuration

After completing the above configuration process, switch to the IVC Console and refresh the **Device Access** page. At this point, the device status will be shown as "online", indicating that the device has been successfully registered and is online.

Audio and Video Configuration Precautions

On the same network, issues such as video stuttering or live broadcast failure often occur due to insufficient or fluctuating network resources. Refer to the following configurations for audio and video parameters.

Note:

- **Do not enable any private encodings from the vendor such as smart264, smart265, SVC, etc., otherwise, registration will fail!**
- **For some vendor devices, modifying the camera configuration under NVR configuration pages may not take effect. It is strongly recommended to log in to the IPC device end for configuration!**

IPC Audio and Video Configuration Specifications

The following diagram uses Hikvision IPC as an example, other vendor devices are similar.

NVR Audio and Video Configuration Specifications

The following diagram uses Hikvision NVR as an example, other vendor devices are similar.

RTMP Protocol Access Practical

Last updated: 2024-08-15 09:54:32

This document will introduce how to access IVC through the RTMP protocol. We will discuss two methods: **Device Streaming and Software Streaming**.

> **Note:**
> You can also watch the RTMP Protocol Access Practical Demonstration Video to understand the overall access process.

1. Camera Streaming Example

1.Create a Device

1. log in to the IVC Console, and select **Device Management** from the left sidebar.
2. First, select the Device Organization, click **Add Device,** and choose the RTMP Protocol.

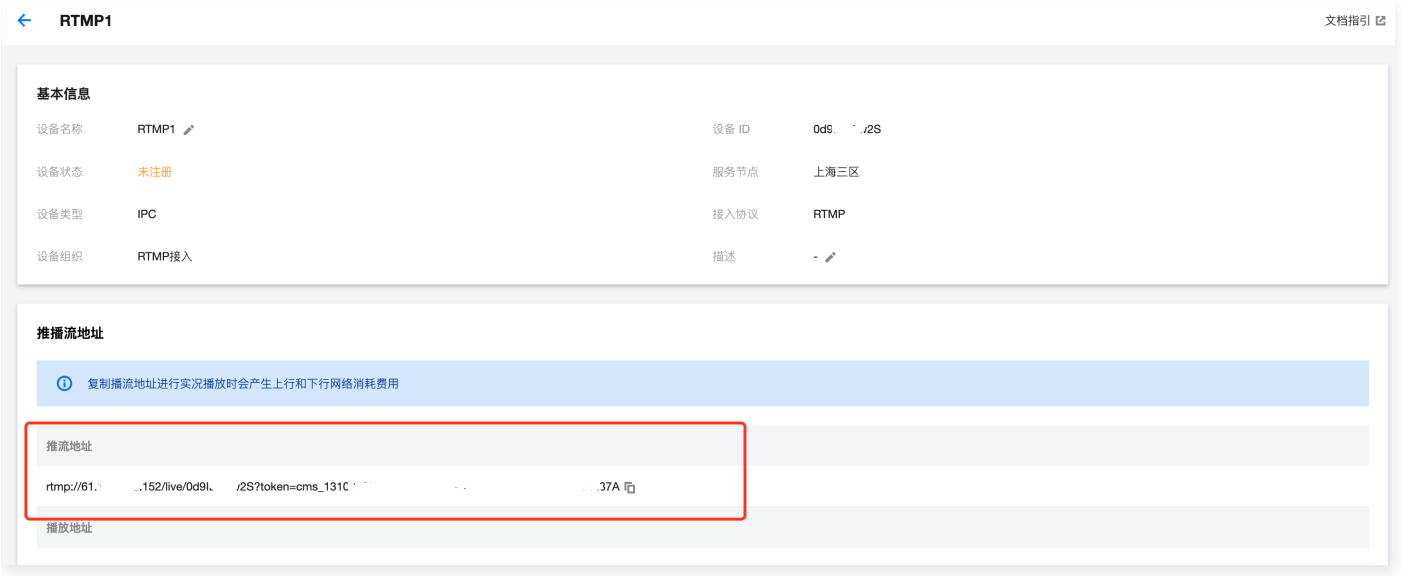
3. You can choose custom {appname} and {streamname} parameters to generate a custom RTMP streaming address.

> **Note:**
> The platform-generated RTMP streaming address format is rtmp://{domain name}/{appname}/{streamname}, all three parameters can be customized.
> - Domain name refers to the domain. You can upload an ICP-registered push domain name as per the page instructions, otherwise, the default will be the platform service's Public IP Address.
> - The app name only supports English, numbers, and must not exceed 32 characters. Otherwise, it defaults to live.
> - The stream name only supports English, numbers, and must not exceed 32 characters. Otherwise, it defaults to a 10-digit device ID generated by the platform.

4. Complete the device addition.

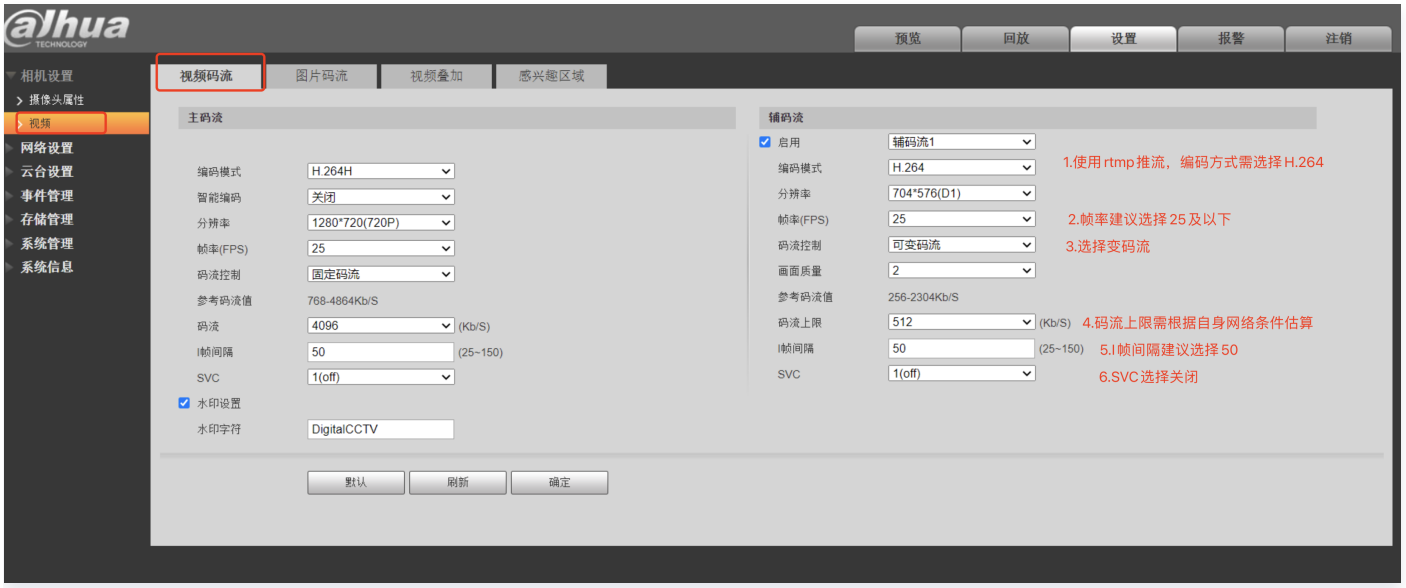
2.Obtain the RTMP Streaming Address

1.Go to the details page of the newly created device to get the streaming address as follows.



3.Device Configuration

1.Log in to the device Web Configuration Page, first configure the audio and video parameters (take Dahua Camera – Auxiliary Stream as an example).



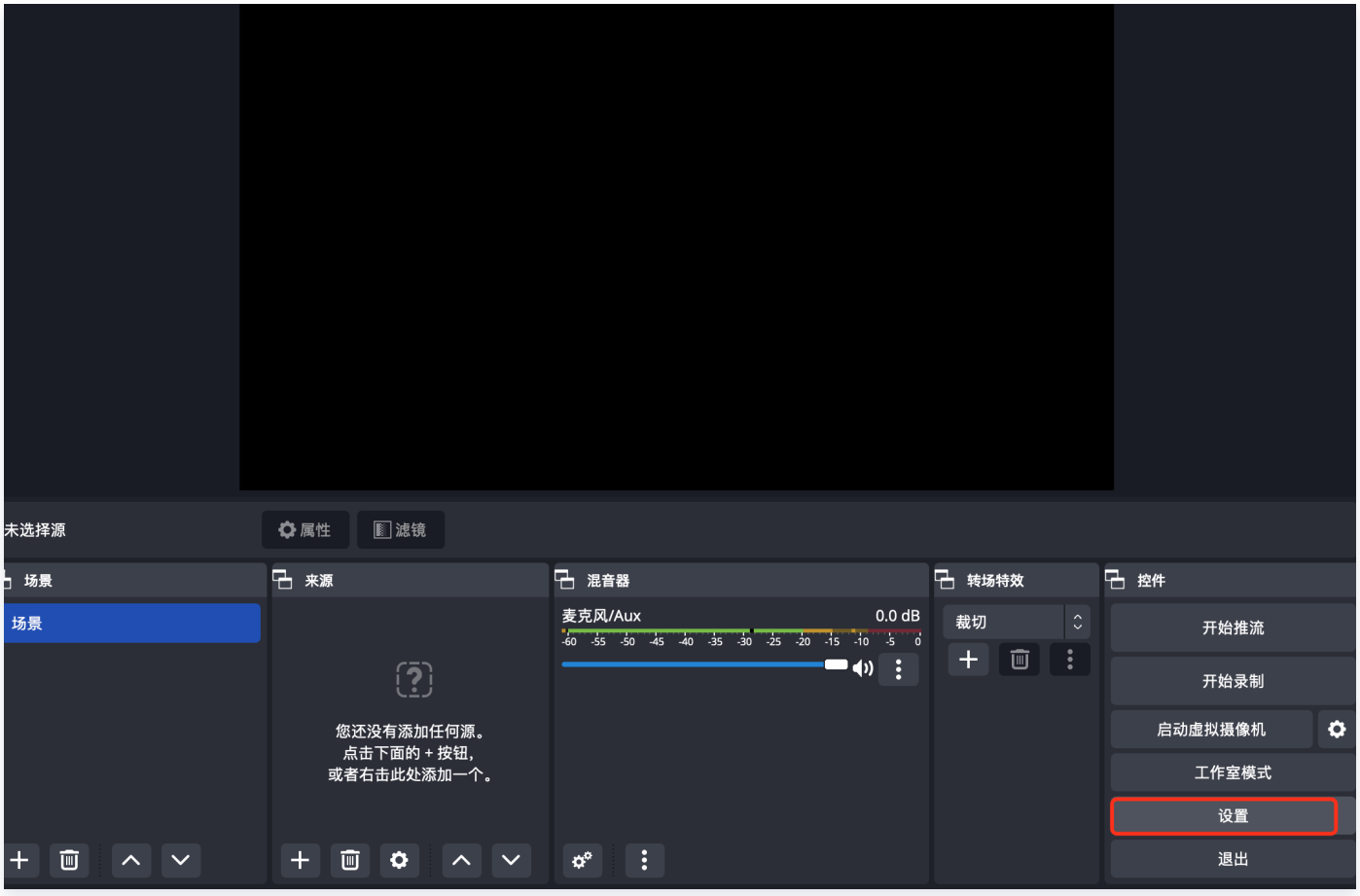
2.Choose **Custom Address Type**, configure the streaming address generated by our platform, and enable streaming.

2. Software streaming example (using OBS Software as an example)

1. Go to OBS official website to download and install.

> **Note:**
> OBS is a free open-source video recording and real-time communication software with multiple features. It is widely used in video capturing and live streaming.

2.Open OBS, click the **widget** in the bottom toolbar> **settings** button to enter the settings interface.



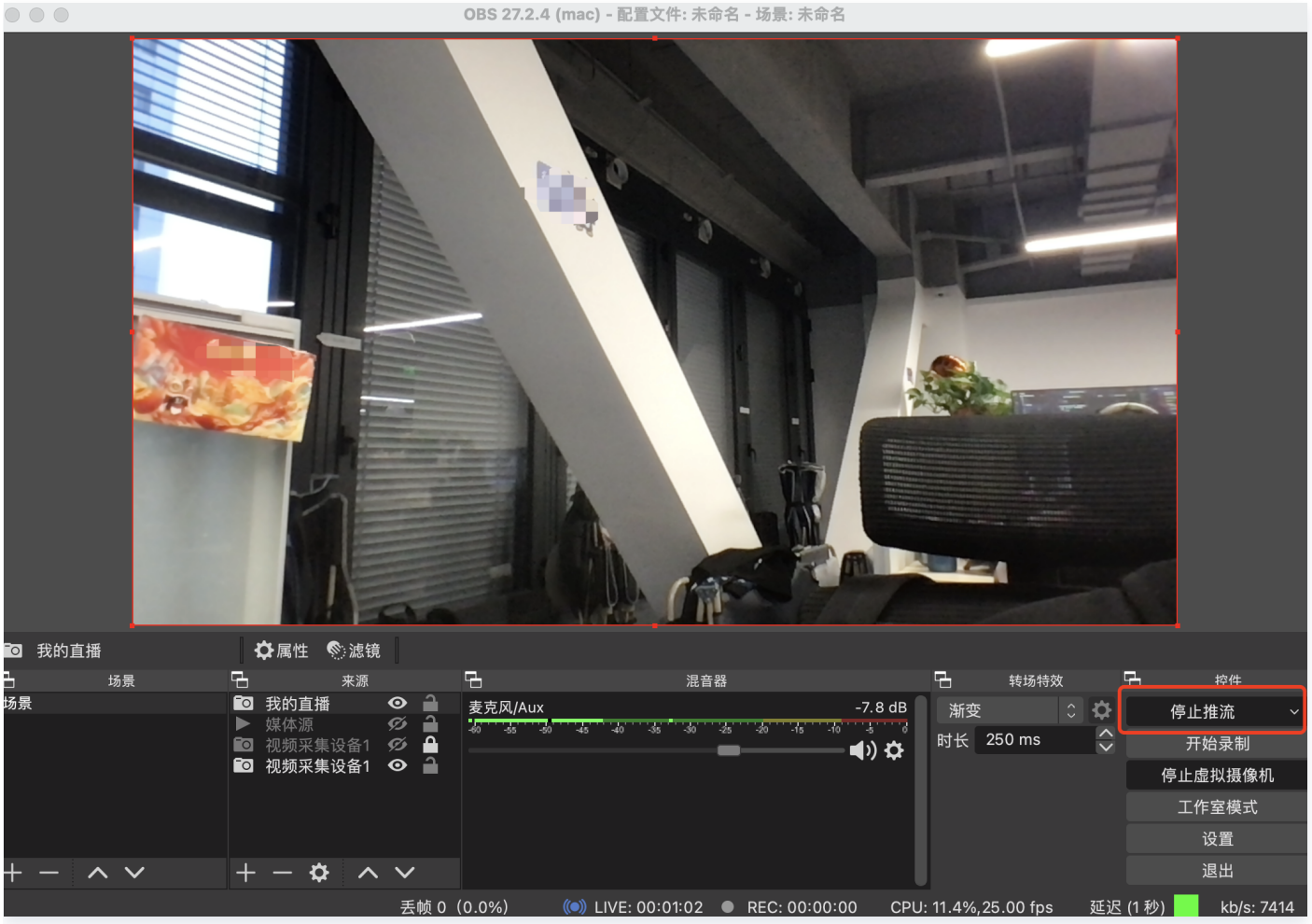
3. click **streaming** to enter the streaming settings page and make the following adjustments.

Note:

- Refer to steps 1 and 2 above for the steps to obtain the streaming address.
- For security, we enable Token Hotlink protection authentication configuration by default for customers. If you do not need it, you can disable it in the **Console – Service Configuration > Authentication Configuration** .

Parameter Configuration	Description
Service Type	Default Self Definition
Server Address	Fill in the server address part of the streaming URL from step 2, for example rtmp://{domain name}/{appname}/
Stream Key	Fill in the stream name and all the contents after it in the streaming URL from step 2, for example {streamname}?token=cms_131...37A

4.Click **Controls > Start Streaming** on the toolbar to start streaming.



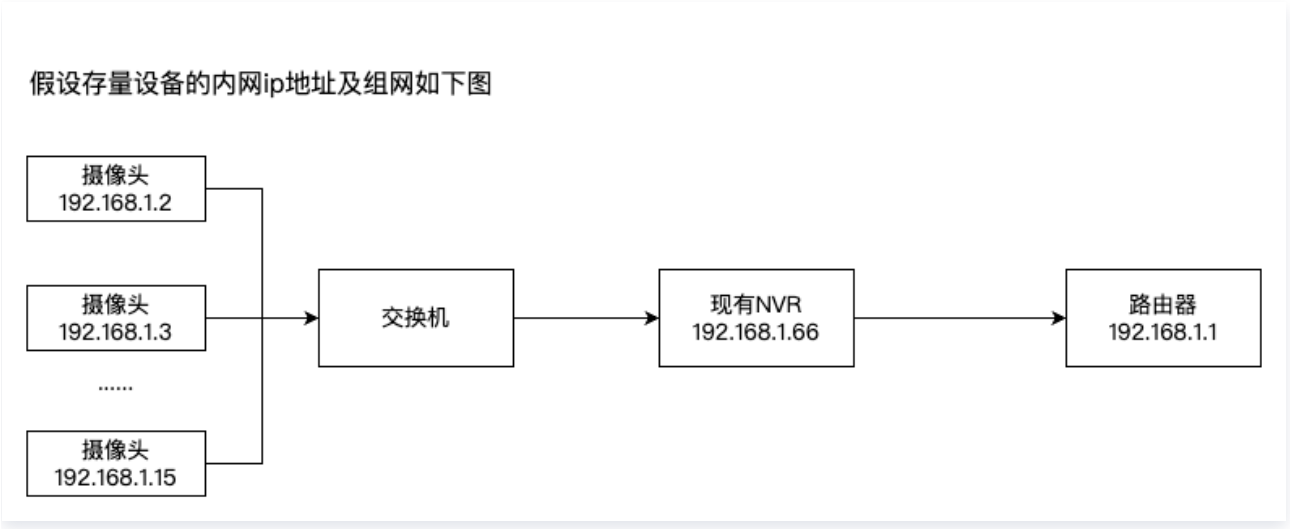
Based on the existing network, add new NVR devices and connect to the platform

Last updated: 2024-08-15 09:59:55

Background

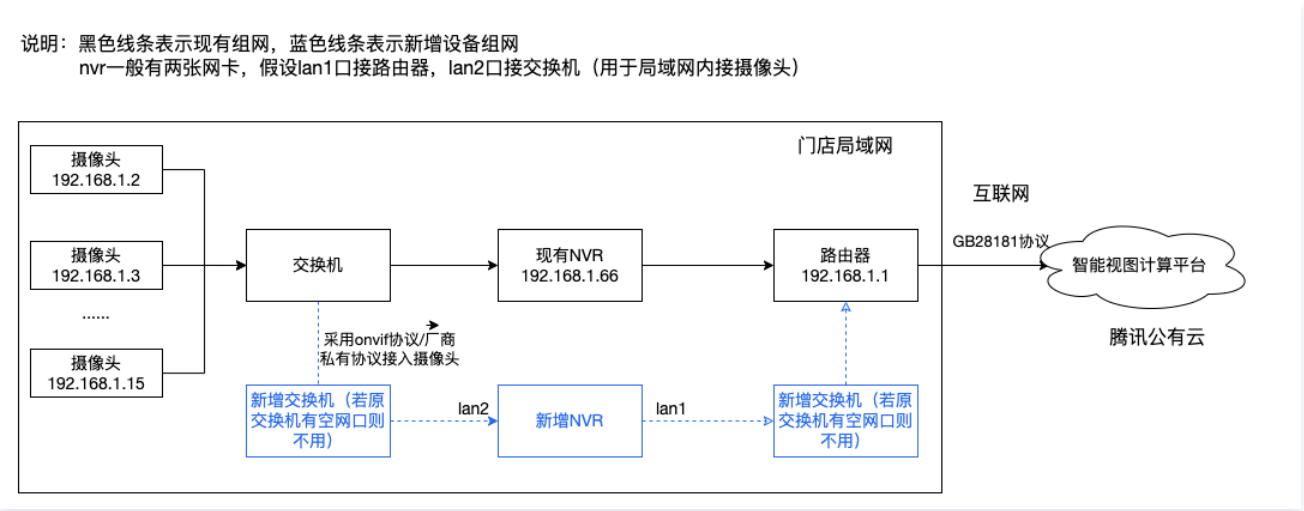
The store already has a video surveillance system (as shown in the network diagram below), with data stored in the NVR Network Video Recorder. With business growth, the customer has proposed the following requirements:

- Storefronts are dispersed nationwide, and the headquarters needs to centralized control to access each storefront's device video at any time.
- The local Digital Video Recorder's storage capacity is insufficient, requiring immediate scale-out to meet the employees' need for retrospective analysis.
- Incidents of equipment theft and data tampering occur frequently, so data needs to be backed up to the cloud, ensuring data integrity and storage reliability in the cloud.
- The current networking setup cannot be changed to avoid impacting existing business operations.



Solution

Based on this context, each storefront needs to add one NVR device to extend the local storage cycle through a bypass grid connection. Simultaneously, this device will achieve nationwide device cloud aggregation via the Internet Access Platform.
manage and back up data to the cloud.



Operation Procedure

Step 1: Install the new device and connect it to the existing cameras

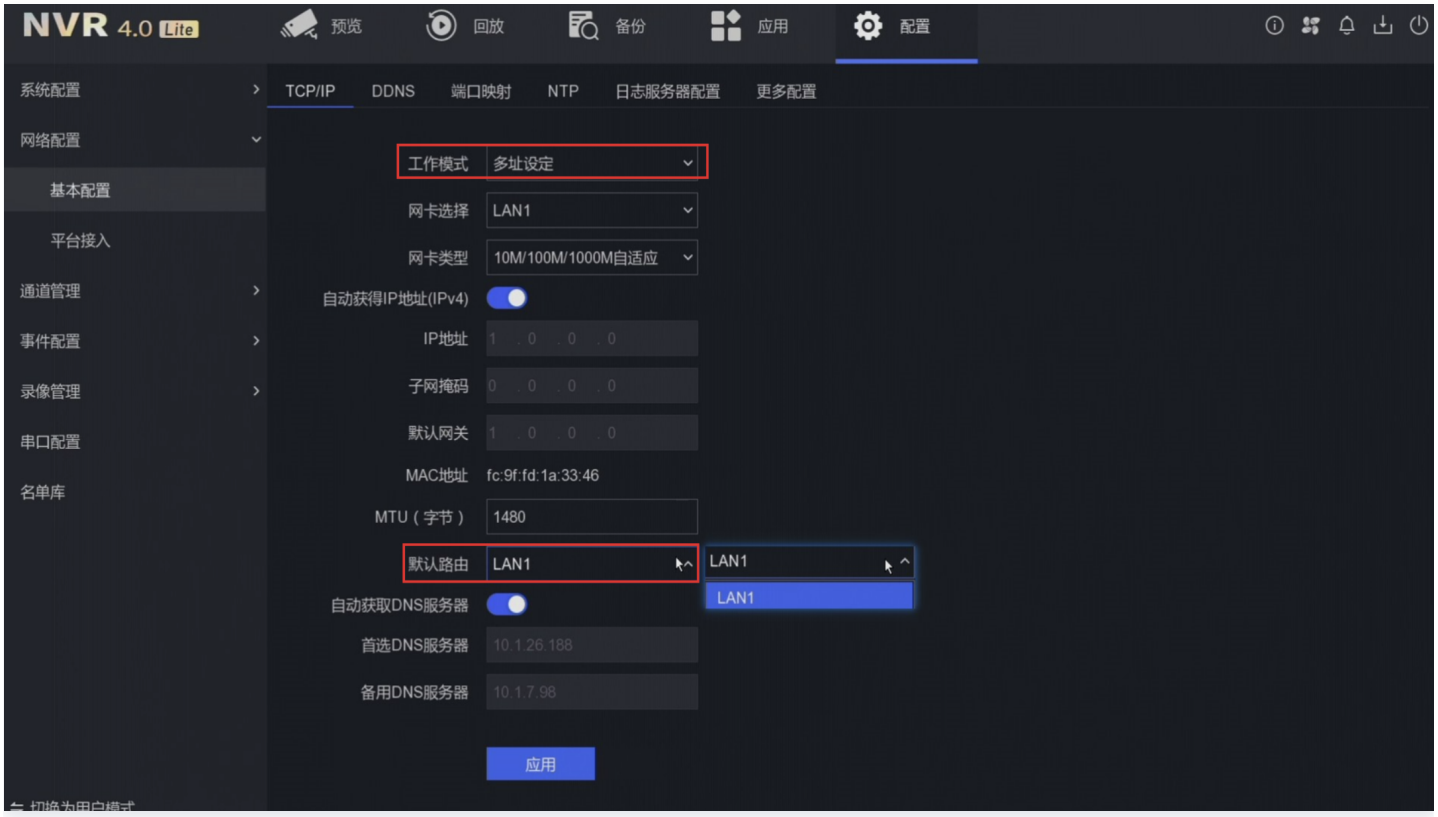
1. Follow the solution by first installing the new NVR (Hikvision in this example) and setting up the network.
2. Determine the new NVR's private IP address and log in to its configuration page.

> **Note:**
> There are three ways to find the device's private IP: using the manufacturer's intranet device search tool, logging in to the router configuration page to find it, or directly connecting a monitor to the new NVR to log in and retrieve it.

3. Configure the device's network parameters

Enter the [Network Settings–Basic Configuration] page, change the Operation Mode to **"Multiple Address Setting"**, select LAN1 for the network card, set LAN1 to automatically obtain an IP address, enable automatic acquisition of DNS servers, select LAN1 for the default route, and click **"Apply"**.

> **Note:**
> - The multiple address setting mode means that the parameters of the two network cards are independent and do not affect each other.
> - The default route means that when the system proactively connects to an external network, the data is forwarded by the default route. Since LAN1 will be used to access the public network, it is chosen as the default route.



Select LAN2 for the network card, assign an internal IP address to LAN2 (for example, 192.168.1.100), and click **"Apply"** after setting.

> **Note:**
> Since LAN2 will connect to cameras within the local area network, it needs to be on the same subnet as the cameras but without IP conflicts; otherwise, the cameras will not be accessible.

4. Connecting Existing Cameras

Enter the [Device Access] page, and the NVR will automatically obtain information on all cameras within the local area network, allowing camera access.
You can choose a suitable protocol for access (generally supports multiple access protocols, for example, onvif); 'password' in the diagram refers to the camera's configuration end login password; the camera has multiple streams, accessing here does not affect its existing surveillance system's streaming.

Step 2: Use the GB28181 Protocol to Access the Cloud Platform

Configure the national standard information on the [Platform Access – GB28181] page to enable new device access to the cloud platform.

> **Note:**
> For step-by-step operation details, please refer to GB/T28181 Protocol Access Practice.

Grant different operational permissions to sub-accounts

Last updated: 2024-08-15 10:00:16

Background

In reality, the root account needs to grant sub-accounts of employees at different levels with product feature operational permissions to meet security compliance requirements. This article will list the practice process of permission authorization under multiple scenarios.

Prerequisites

- Tencent Cloud accounts are managed in Tencent Cloud Certificate Authority M CAM (Cloud Access Management). You need to understand the basic concepts of sub-accounts, permissions, policies, etc., in advance. Please refer to CAM Operation Guide .

Among them, a policy is a collection of one or more operational permissions, categorized as follows:

	Creator	Application scenario	Predefined policies for this product	Description
Preset Policy	Various products of Tencent Cloud	A collection of frequently used product feature permissions	QcloudISSReadOnlyAccess IVC (ISS) Read-only Access Permission	Users can only view, not modify
			QcloudISSFullAccess IVC (ISS) Full Read-Write Access Permission	Users can fully operate and view
Custom Rules	User	Refined permission management, where users can create based on business scenarios themselves	No	No

- For the complete process of executing sub-account permission authorization, please refer to User Permissions .

Scenario One: Authorize sub-accounts with full operational permissions

Applicable to: Headquarters operation and maintenance team, headquarters digital department (responsible for undertaking video business)
Scenario: This type of sub-account coordinates the overall business (acting as the role of a super administrator),
Authorization policy: The master account authorizes the sub-account with preset product policies: **QcloudISSFullAccess** IVC (ISS) full read/write access.

> **Note:**
> This type of sub-account can create multiple sub-accounts for regional personnel. It needs to be granted the **QcloudCamFullAccess** preset strategy. Then, the sub-account can be created.

Scenario 2: Sub-accounts can only view device status and recordings, without any edit operations

Applicable to: Sub-accounts of regional personnel
Scenario: In coordination with headquarters personnel to troubleshoot equipment failures and routinely access videos of devices within their responsible region. Therefore, they can only live preview and playback recordings (local, cloud) of authorized devices, unable to edit device organization, add/delete devices, download cloud recordings, etc., nor can they view other features.
Authorization policy: Is required to be created by the master account with custom Definition policies (must include the following product interfaces). For details, please refer to Custom Definition Policy Creation Guide. Finally granted to the sub-account.

API Name	Interface description
DescribeOrganization	Query Organization
DescribeDeviceChannel	Query Device Channel
DescribeDeviceRegion	Query All Device Service Nodes
DescribeDictionary	Get Dictionary
DescribeRecordPlaybackUrl	Get Cloud Recording Playback URL
DescribeUserDevice	Query Device
ListDevices	Get Device List
DescribeRecordFile	Recording File Retrieval
ControlDeviceStream	Get Streaming Address
ControlRecord	Recording Control
ControlRecordTimeline	Request Recording Timeline

PlayRecord	Recording Playback
RefreshDeviceChannel	Refresh Device Channel
ListTasks	Queries the list of tasks

Viewing Sub-account Operation Logs

Last updated: 2024-08-15 10:01:12

Background

When employees use a Tencent Cloud sub-account to log in to the console or use the TencentCloud API to access resources under the main account, you may need the following information:

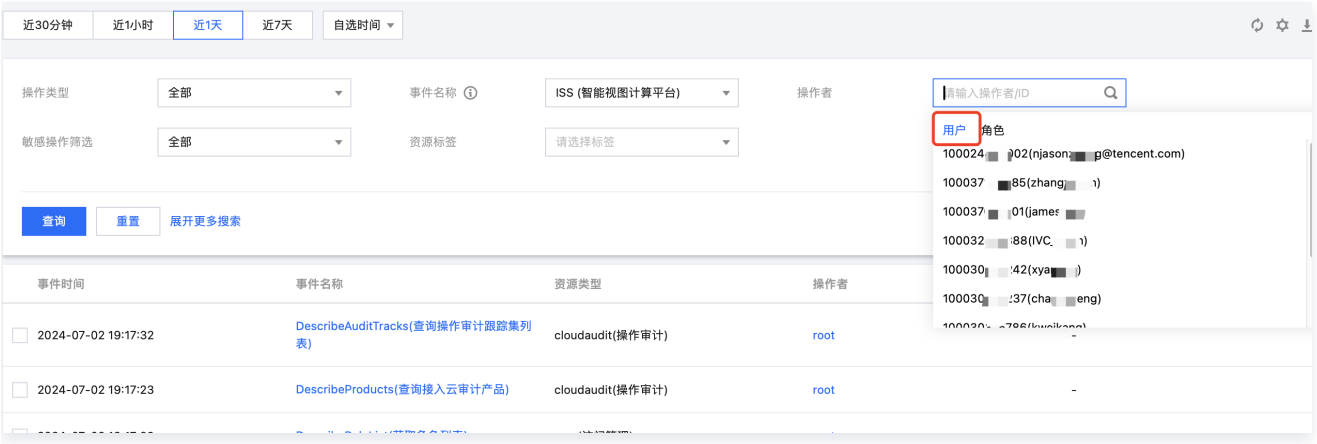
- What resources did the employees access?
- How do I check the modification records of resource configurations?
- Are employees accessing Tencent Cloud within the environment you specified?

At this time, you can view and track employees' operation logs through the CloudAudit product. CloudAudit supports the online viewing of operation records on the Tencent Cloud console and TencentCloud API within 90 days.

Operation step

1.Log in to the CloudAudit console, click on the Operation Records feature. Select the event name "IVC"

2.You can view the operation logs of sub-accounts by filtering through the "Operator".



3.Click the event details to view information such as the operator's source IP address and sub-account ID.

Shipping Log with Tracking Set

If you need to view employee operation records for a longer period, you can use CloudAudit's Tracking Set feature to deliver logs to a COS bucket or CLS.
When delivering to CLS, you can select specific operations of this product (such as sensitive operations) and configure alarm strategies in CLS. For detailed operations, please refer to Using Log Delivery for Tracking Sets.