Live

Interactive Live Streaming

Issue 01

Date 2024-12-16

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Overview

Cloud Live is an easy-to-use livestreaming service that provides diverse live acceleration capabilities for entertainment, e-commerce, and education scenarios.

It includes the following subservices:

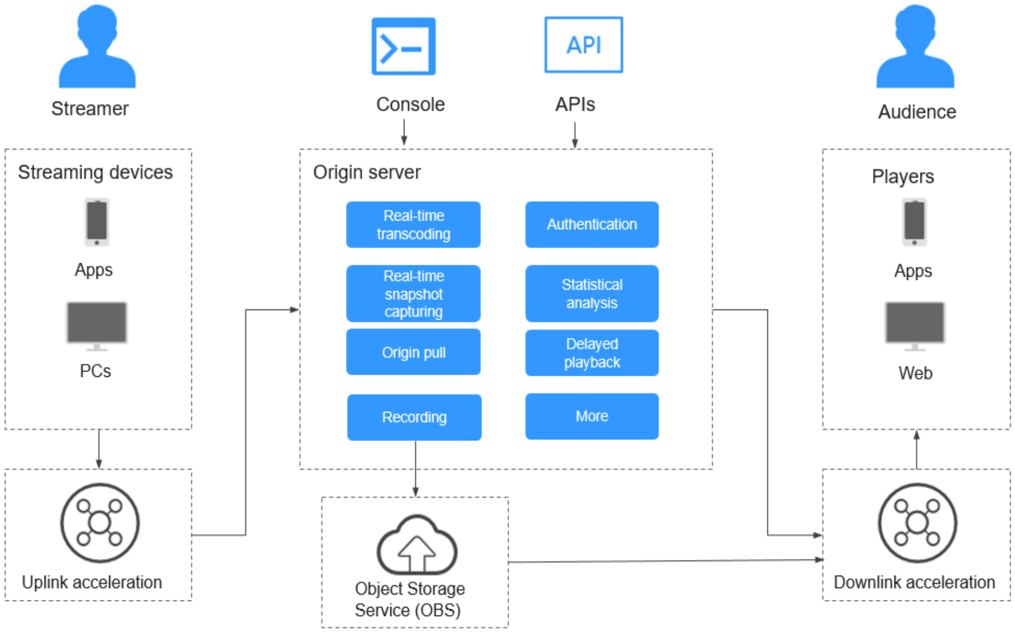
- Cloud Stream Live improves the stability and efficiency of high-concurrency livestreaming and provides powerful real-time media processing capabilities.
- Low Latency Live (LLL), which is built on cutting-edge technologies such as transmission protocol optimization, dynamic routing, and low-latency transcoding, slashes live latency to milliseconds in latency-sensitive scenarios and delivers an unrivaled experience even when there are a massive number of concurrent requests.

NOTE

For details about how to enable Live, see **Getting Started**.

Service Architecture (for Cloud Stream Live)

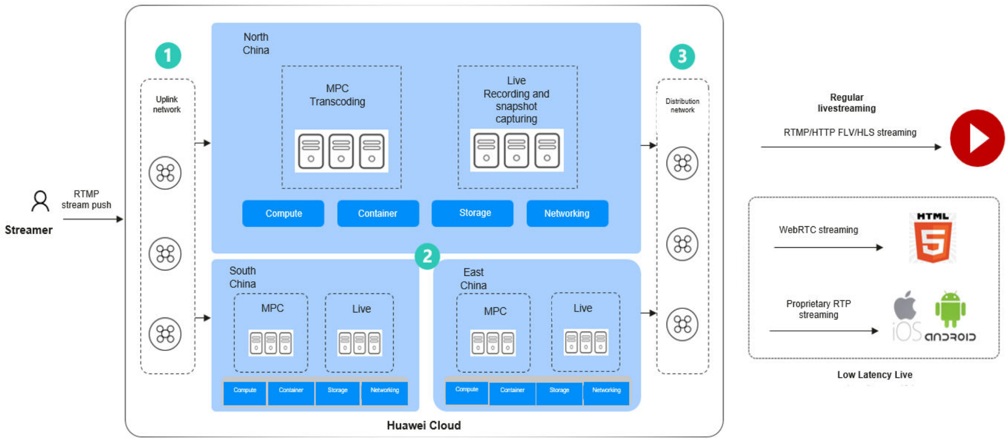
Figure 1-1 Service architecture



Process of livestreaming:

1. A streaming tool is used to push a livestream to an origin server with uplink acceleration enabled.
2. The origin server transcodes the livestream in real time.
3. The processed livestream is distributed to viewers with downlink acceleration enabled.
4. Live records the livestream to Object Storage Service (OBS).

Service Architecture (for LLL)



Features

Global acceleration

2,800+ nodes are deployed worldwide and provide a bandwidth reserve of more than 100 Tbit/s.

Ultimate experience

Supports tens of millions of concurrent requests. Huawei-developed congestion control algorithm and intelligent scheduling policy secure ultra-HD and smooth livestreaming, with a frame freezing rate lower than 1%. Low-bitrate HD transcoding is more suitable to human eyes-based subjective rate-distortion decision model and reduces the bitrate by 30% to 40% whereas the video subjective quality does not deteriorate.

High stability & reliability

Provides multi-center and cross-region cluster disaster recovery and 24/7 service support. The livestreaming architecture is built on Huawei's 20 years of Cloud Native 2.0 experience. It is an agile and intelligent architecture that combines enhanced security and reliability with fast scaling to safeguard your livestreaming.

Statistical analysis

Provides statistics about livestreaming, value-added services, and stream playback profiles. All access logs can be downloaded, facilitating service analysis and service development.

Demo

A multi-terminal demo is provided for you to try out LLL.

To obtain the app demo and source code, contact Huawei Cloud technical engineers by **submitting a service ticket**.

Pricing

By default, the fee is charged by downlink playback traffic. Currently, you can pay by traffic, daily peak bandwidth, or 95th percentile bandwidth. For details, see **Billing**.

2 Scenarios

Application scenarios of Cloud Live:

- **Cloud Stream Live**
- **LLL**

Cloud Stream Live

Online education: Cloud Stream Live is an easy-to-integrate cloud service that can guarantee low-latency HD even when there are a massive number of viewers. Powerful real-time media processing ensures that videos can be quickly sent to interactive education websites. The acceleration nodes networkwide allow students to watch smooth videos. With video recording and transcoding, students can review learning materials at any time. In addition, hotlink protection prevents teaching materials from unauthorized use to protect copyrights.

Interactive entertainment: Cloud Stream Live can be used for livestreaming by influencers and enterprises, or livestreaming for entertainment and gaming. Diverse media processing functions are provided, such as real-time transcoding and inappropriate content identification, to build a one-stop E2E livestreaming solution.

Live commerce: Cloud Stream Live helps e-commerce platforms better present their products to turn more prospects into customers. The ultra-low latency keeps both streamers and viewers informed of transactions in real time so that viewers can buy products while watching the video.

Live events: Cloud Stream Live enables you to manage permissions for playing video using IP address access control lists (ACLs), URL validation, and the Advanced Encryption Standard (AES). These features help protect live content from unauthorized playback. Live video recording and recording file index creation are supported. Together with VOD, a one-stop Live-to-VOD solution is provided to facilitate the livestreaming of sports games, e-games, and enterprise presentations.

LLL

Large online courses: Millisecond-level latency facilitates interactivity in class, such as smoother Q&A sessions and whiteboard sharing, significantly improving student engagement and learning efficiency.

Live commerce: Low latency ensures a fair and consistent experience in live commerce activities such as flash sales. The streamer can answer viewers' questions and on-screen comments in a timely manner, attracting more visitors to the e-commerce platform for higher gross merchandise volume (GMV).

Fashion shows: The streamer can receive gifts sent by viewers and answer their questions immediately, improving interactivity in this latency-sensitive scenario.

Live sports: Fans can watch sports games together in a live room and interact with each other in real time at a low latency.

3 Functions

Huawei Cloud Stream Live provides a wide range of livestreaming functions, such as stream push, live video playback, recording, and transcoding. These functions make the service an ideal option for many latency-sensitive scenarios, such as online education and interactive entertainment. See **Table 3-1**.

📖 NOTE

HTTPS is recommended, as it is more secure than HTTP.

Table 3-1 Functions

Type	Function	Description
Stream push	Protocol	RTMP push and streaming audio or video
	Method	Stream push using third-party software such as Open Broadcaster Software, XSplit, and FMLE
	Uplink acceleration	Supports uplink acceleration, user access point/ device scheduling (DNS/HTTP DNS), access control, and auto scaling for live video.
Livestreaming	Protocol	● Cloud Stream Live: RTMP, HTTP-FLV, and HLS ● Low Latency Live: WebRTC, which can be downgraded to HTTP-FLV
	Method	● Cloud Stream Live: playback using third-party software such as VLC ● Low Latency Live: playback on web clients using the LLL online demo or API
	Downlink acceleration	Supports downlink acceleration, user access point/device scheduling (DNS/HTTP DNS), access control, and auto scaling for live video.
Stream processing	Recording	You can record a livestream in HLS, FLV, or MP4 format and store the recordings in OBS.

Type	Function	Description
	Transcoding	You can transcode a livestream into different specifications using H.264, H.265, or low-bitrate HD transcoding.
	Snapshot capturing	You can capture snapshots from a livestream and save JPG snapshot files in OBS buckets.
	Delay	You can change the playback delay. **NOTE** This function is not recommended for LLL.
	Origin pull	You can pull live content from your own origin server to a Huawei Cloud origin server for accelerated delivery.
Streaming	Management	You can manage livestreams on the Live console or by calling APIs.
Live console	Dashboard	● You can view the downstream traffic and peak downstream bandwidth on the current day. ● You can change the CDN billing option.
	Streaming	You can view ongoing streams and disabled streams.
	Domain name management	● You can add, delete, disable, and enable ingest domain names and streaming domain names. ● You can associate an ingest domain name with or disassociate it from a streaming domain name. ● You can configure transcoding, snapshot capturing, and stream status notifications for ingest domain names, and stream push authentication. ● You can configure the origin pull settings, HTTPS certificate, latency, URL validation, referer validation, and access control lists (ACLs) for streaming domain names.
	Usage Statistics	You can view the downstream bandwidth/traffic statistics of all streaming domain names, and the total transcoding duration, maximum number of concurrent recording channels, and number of snapshots of all ingest domain names.

Type	Function	Description
	Service monitoring	You can view the downstream bandwidth/traffic, playback profile, status codes returned in the request response of a streaming domain name, and the number of online viewers of the corresponding livestream. You can also view monitoring information such as the upstream bandwidth/traffic, total number of pushed streams, and stream push frame rate/bitrate of an ingest domain name.
	Log management	You can view logs about requests to a streaming domain name and download logs over the past 14 days.
	OBS authorization	You can authorize Live to store captured snapshots in OBS buckets.
	Tools	You can quickly generate signed URLs for streaming and ingest domain names.
Access control	URL authentication	You can configure an authentication key to verify requests.
	Referer validation	You can configure a referer blacklist to identify and filter out unauthorized access.
	Access control list (ACL)	You can configure an IP address blacklist to identify and filter out unauthorized access.
	HTTPS secure acceleration	You can use the certificate of a streaming domain name to configure and deploy HTTPS for all CDN nodes on the network to secure livestreaming acceleration.
APIs	Domain name management	● You can create, delete, modify, and query domain names. ● You can create and delete the mapping between a streaming domain name and an ingest domain name.
	Transcoding	You can query, modify, create, and delete transcoding templates.
	Streams	You can query and modify the status of streams and query live acceleration data.
	Access control	You can query, update, and delete the URL validation configuration of a specified domain name.
	Snapshot management	You can create, delete, modify, and query snapshot capturing templates.
	Log management	You can query livestreaming logs.

Type	Function	Description
	Recording management	You can create, query, and delete recording templates, and record livestreams to OBS.
	Recording callback management	● You can create, delete, and modify a recording callback, and query details of a recording callback. ● You can query the list of recording callbacks.
	HTTPS certificate management	You can query, modify, and delete the HTTPS certificate settings of a specified domain name.
	OBS bucket management	You can grant or cancel authorization of accessing OBS buckets.
	Statistical analysis	You can query traffic or bandwidth data, and peak bandwidth in a specific period.
	Stream analytics	You can view the frame rate and bitrate of a single livestream.
SDK	Server SDK	SDK helps you perform secondary development. The supported languages are: Java, Python, Go, and PHP.

4 Advantages

Advantages of of Cloud Live:

- Cloud Stream Live
- LLL

Cloud Stream Live

Livestreaming acceleration: RTMP stream push and RTMP/HTTP-FLV/HLS stream pull are supported. With intelligent scheduling, streams can be pushed to the site nearby, delivering a frame freezing rate lower than 2.5%. A playback success rate of more than 99.9% ensures instant video playback.

Low-bitrate HD: Lower bitrate at a given image quality reduces bandwidth costs by 20–30%.

High cost-effectiveness: H.264/265 transcoding and FPGA-based hardware acceleration improve livestreaming experience and greatly reduce costs.

Enhanced security & reliability: Cross-region DR and 24/7 technical support safeguard your business.

LLL

Millisecond-level latency: UDP is used to livestream within milliseconds in high-concurrency scenarios, which outperforms regular livestreaming that suffers from a latency of 3–5 seconds. In addition, core metrics such as first-frame latency and frame freezing rate are improved, minimizing livestreaming latency for viewers.

Comprehensive functions and high compatibility: LLL supports major functions of Cloud Stream Live, such as stream push, live transcoding, recording, snapshot capturing, pornographic identification, and playback. You can easily migrate your workloads from Cloud Stream Live to LLL.

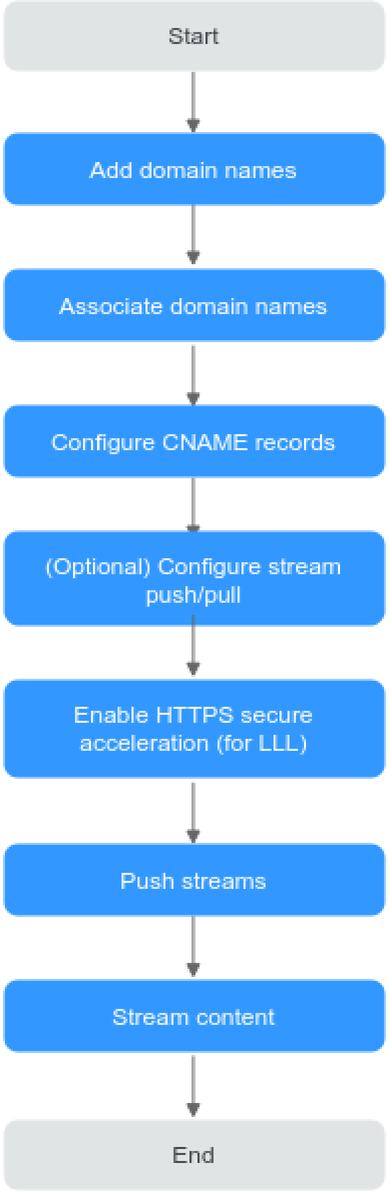
Easy usage and enhanced security: Using standard protocols allows playing video on Chrome and Safari with no need for plug-ins. Protocols are encrypted by default, which are secure and reliable.

5 Getting Started

5.1 Quick Start

If you want to use Cloud Live with your own domain names, see **Figure 5-1**.

Figure 5-1 Getting started with Cloud Live



For details, see **Table 5-1**.

Table 5-1 Getting started with Cloud Live

No.	Operation	Description
1	**Adding domain names**	Add an ingest domain name and a streaming domain name to Live. You can register a level-1 domain name (for example, example.com) and use two level-2 domain names (for example, live-play.example.com and live-push.example.com) as the ingest domain name and streaming domain name.

No.	Operation	Description
2	**Associating domain names**	Associate the ingest domain name with the streaming domain name. Otherwise, the playback will fail.
3	**Configuring CNAME records**	Live assigns a CNAME record to the ingest domain name and streaming domain name. Configure the CNAME records at your domain names' DNS providers to enable livestreaming acceleration.
4	**Enabling HTTPS secure acceleration**	You can enable HTTPS secure acceleration for LLL to ensure that your live content is encrypted during transmission. This operation is required only for LLL.
4	- (Optional) Configuring stream push – **Transcoding** – **Recording** – **Snapshot capturing** – **Stream authentication** - (Optional) Configuring stream pull – **Stream delay** – **Origin pull** – **HTTPS secure acceleration** – **Playback authentication**	Configure recording, transcoding, snapshot capturing, and authentication before streaming.
5	Pushing streams	You can use a third-party streaming tool such as Open Broadcaster Software (OBS) to push streams. - Cloud Stream Live: **Pushing Streams** - LLL: **Pushing Streams**

No.	Operation	Description
6	Streaming content	● Cloud Stream Live: You can use a third-party player such as VLC media player to stream content. See **Streaming Content**. ● LLL: You can play a video on web clients through the Huawei Cloud LLL online demo or API. See **Streaming Content (on a Web Client)**.

5.2 Adding Domain Names

This section describes how to add an ingest domain name and a streaming domain name.

Prerequisites

- You have registered with Huawei Cloud and completed real-name authentication.

  NOTE

  If you are a user of Huawei Cloud (International) or Huawei Cloud (Europe), you need to complete real-name authentication when you:

  - Purchase and use cloud services in Huawei Cloud regions in the Chinese mainland. In this case, real-name authentication is required by the laws and regulations of the Chinese mainland.
  - Plan to use Live in Huawei Cloud regions in the Chinese mainland.

- Domain names for Live are available. Live requires an ingest domain name and a streaming domain name, and the two domain names must be different.

  NOTE

  If you want to perform livestreaming acceleration in Huawei Cloud regions in or outside the Chinese mainland, the domain names must complete ICP filing in advance as required by the Ministry of Industry and Information Technology (MIIT).

- You need to prepare an HTTPS certificate before using LLL.
  - If you do not have an HTTPS certificate, you can purchase one on Huawei Cloud **SSL Certificate Manager**.
  - The HTTPS certificate format must meet the **requirements**. If your certificate is not in PEM format, **convert the certificate** to the PEM format.

Notes

- An area needs to be specified for stream push, and the streaming domain name needs to be associated with an ingest domain name. In this way, a streaming domain name can be used to watch livestreaming in the area where the ingest domain name is located. That is, a streaming domain name cannot be used to watch livestreaming in and outside China at the same time.

- The price of livestreaming outside China is different from that in China. For details, see **Pricing Details**.
- If the streaming URL is not used in the selected acceleration area, the playback quality may be compromised.
- If the **Service Area** of the streaming domain name is **Chinese mainland** or **Global**, and the origin server of the ingest domain name is in the Chinese mainland, the domain names must be licensed in the Chinese mainland.
- If you add, modify, or delete a domain name, the change will be displayed in My Resources within 24 hours. Please check the data later.

Adding Domain Names

Add the ingest and streaming domain names to Live. The following describes how to add an ingest domain name. The procedure for adding a streaming domain name is the same.

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Add Domain**. On the displayed page, enter an ingest domain name.

Table 5-2 Domain name parameters

Parameter	Description
Domain Name	Enter a second-level ingest domain name or streaming domain name, for example, test-push.example.com. **NOTE** ● The domain name can contain a maximum of 64 characters, which cannot contain uppercase letters. ● An ingest domain name must be different from a streaming domain name. Wildcard domains are not allowed. ● By default, you can add up to 64 domain names in your account. To add more domain names, **submit a service ticket**.
Enterprise Project	Add domain names to enterprise projects for unified management. On the **Create Enterprise Project** page, **create an enterprise project** (whose name is **default** by default) and **add the user group to the enterprise project**. By doing so, users in this user group obtain the permissions on the domain names in the enterprise project. **NOTE** Only an enterprise account can configure enterprise projects.
Type	If you enter an ingest domain name for **Domain Name**, then select **Ingest domain name** for **Type**. The domain name type cannot be changed once configured.

Parameter	Description
Live Origin Server	Area where the Live origin server is located. For details, see How Do I Select a Live Origin Server and Acceleration Area? The Live origin server cannot be changed once configured. Select the nearest origin server. Currently, Live origin servers are deployed in the following regions: ● CN North-Beijing4 of Huawei Cloud (Chinese Mainland): CN North-Beijing4 and AP-Singapore. ● Singapore of Huawei Cloud (International): AP-Singapore, LA-Sao Paulo1, and CN North-Beijing4. ● Dublin of Huawei Cloud (Europe): EU-Dublin. **NOTE** ● The origin server of the ingest domain name must be in the region where the streamer is. Streamers cannot push streams across regions. For example, if a streamer needs to livestream in both the Chinese mainland and Malaysia, two sets of streaming and ingest domain names need to be configured. The origin servers of each set of domain names are located in the Chinese mainland and Singapore, respectively. ● The origin servers of the ingest and streaming domain names to be associated must be in the same region. ● The OBS buckets that you use for storing live video recordings and snapshots must be in the same region as the Live origin server.
Service Area	Area where streaming domain names can be accelerated. For details, see How Do I Select a Live Origin Server and Acceleration Area? This parameter is valid only for streaming domain names and cannot be changed once configured. If the video is not played in the selected acceleration area, the livestreaming quality may be compromised. Select an acceleration area that fits your needs. Options: ● **Europe** Select this option when the audience is in Europe. ● **Global** Select this option when the audience is not in Europe. If you select **Global** as the acceleration area, when you or your end users use the domain name, the configuration data of the domain name, including audio and video data, may be transferred across borders in the following scenarios: ● Audio and video data is transferred across borders from Ireland to the country or region where your end users are. ● The configuration data of the domain name is transferred from Ireland to Singapore. **NOTICE** If the **Service Area** you select involves cross-border data transfer, you shall be responsible for such transfer. For details, see section 2.3 "Processing Your Content Data" of **Live Service Agreement**.

Parameter	Description
Supported Protocol	Streaming protocols supported by a streaming domain name. ● This parameter is valid only for streaming domain names. ● The value defaults to **FLV+RTMP+RTC** and cannot be changed once specified. Options: ● **FLV+RTMP+RTC**: The streaming domain name can use HTTP-FLV, RTMP, and WebRTC to play Cloud Live content. ● **HLS**: The streaming domain name can use HLS to play Cloud Live content.

Step 4 Click **OK**.

A domain name whose **Status** is **Configuring** is displayed in the domain name list. About 3 to 5 minutes later, if the status becomes **Normal**, the domain name has been added.

Step 5 Repeat **step 1** to **step 4** to add a streaming domain name.

After adding the streaming domain name, you need to associate the streaming domain name with the ingest domain name before using Live. The associated ingest domain name and streaming domain name must belong to the same Live origin server. For details, see **Associating Domain Names**.

----End

Associating Domain Names

Associate the ingest domain name with the streaming domain name so that you can push streams and play live video.

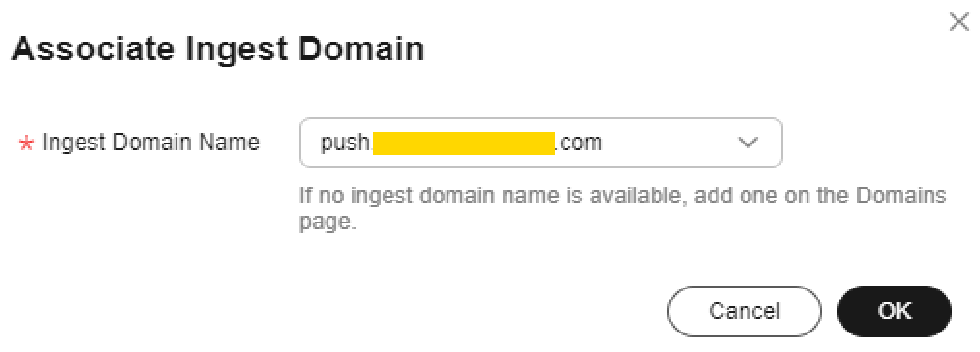
Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Manage** in the row containing the target streaming domain name. The **Basic Info** page is displayed.

Step 4 In the **Ingest Information** area, click **Associate Ingest Domain** and select the added ingest domain name.

Figure 5-2 Associating domain names



Associate Ingest Domain

* Ingest Domain Name: push[redacted].com

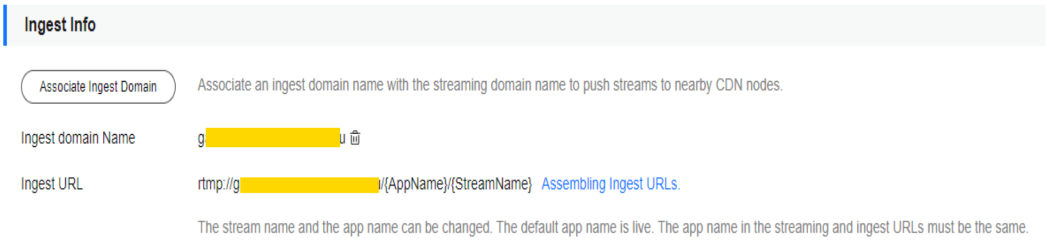
If no ingest domain name is available, add one on the Domains page.

Cancel | OK

Step 5 Click **OK**.

Then you can view the stream push information in the **Ingest Info** area.

Figure 5-3 Ingest Info



Ingest Info

Associate Ingest Domain — Associate an ingest domain name with the streaming domain name to push streams to nearby CDN nodes.

Ingest domain Name: g[redacted]u

Ingest URL: rtmp://g[redacted]/{AppName}/{StreamName} Assembling Ingest URLs.

The stream name and the app name can be changed. The default app name is live. The app name in the streaming and ingest URLs must be the same.

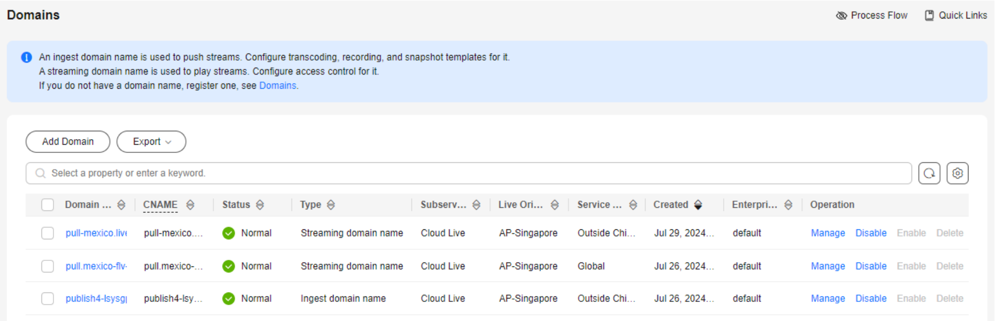
----End

Configuring CNAME Records

After domain names are added, a CNAME record will be assigned to the ingest domain name and streaming domain name, respectively. You can log in to the and view the domain names on the **Domains** page, as shown in **Figure 5-4**.

Configure the CNAME records at your domain names' DNS providers. After the CNAME records take effect, all requests of your ingest domain name and streaming domain name are redirected to CDN PoPs of Huawei Cloud Live for faster livestreaming.

Figure 5-4 Domains



Domains

Process Flow Quick Links

An ingest domain name is used to push streams. Configure transcoding, recording, and snapshot templates for it.
A streaming domain name is used to play streams. Configure access control for it.
If you do not have a domain name, register one, see Domains.

Add Domain | Export

Select a property or enter a keyword.

Domain ...	CNAME	Status	Type	Subserv...	Live Ori...	Service ...	Created	Enterpri...	Operation
pull-mexico.live	pull-mexico....	Normal	Streaming domain name	Cloud Live	AP-Singapore	Outside Chi...	Jul 29, 2024...	default	Manage Disable Enable Delete
pull.mexico-flv-	pull.mexico-...	Normal	Streaming domain name	Cloud Live	AP-Singapore	Global	Jul 26, 2024...	default	Manage Disable Enable Delete
publish4-lsysgi	publish4-lsy...	Normal	Ingest domain name	Cloud Live	AP-Singapore	Outside Chi...	Jul 26, 2024...	default	Manage Disable Enable Delete

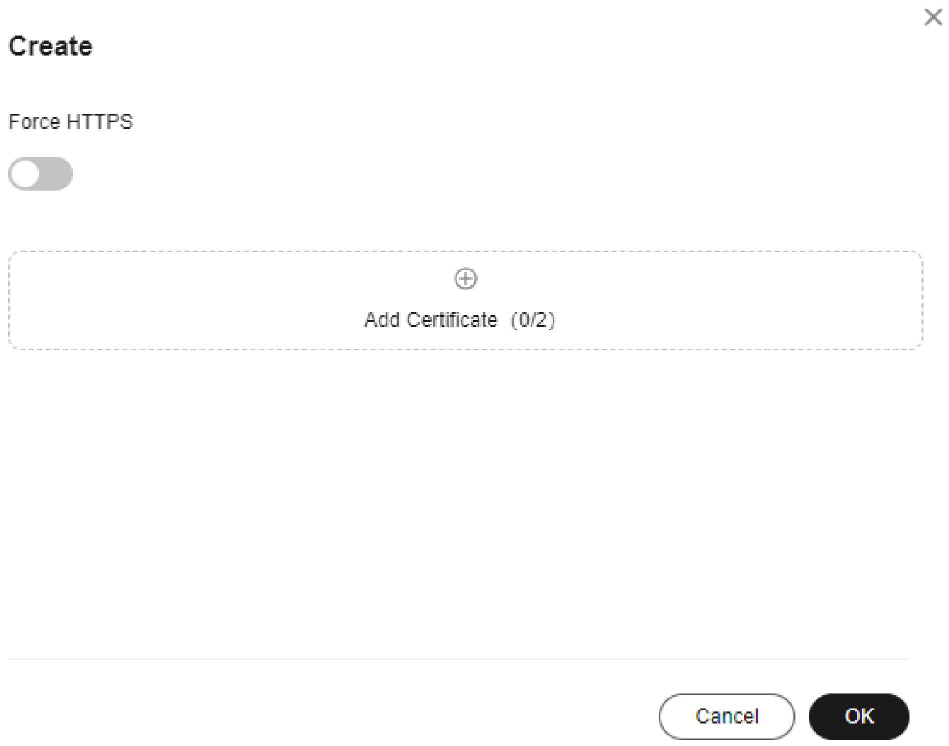
Enabling HTTPS Secure Acceleration

This operation is required only for LLL.

You can enable HTTPS secure acceleration for streaming domain names of LLL to ensure that your live content is encrypted during transmission.

1. Log in to the **Live console**.
2. In the navigation pane, choose **Domains**.
3. Click **Manage** in the **Operation** column of the desired streaming domain name.
4. In the navigation pane, choose **Templates** > **HTTPS Certificates**.
5. Click **Create**. The page of creating certificate settings is displayed, as shown in **Figure 5-5**.

   Figure 5-5 Creating certificate settings

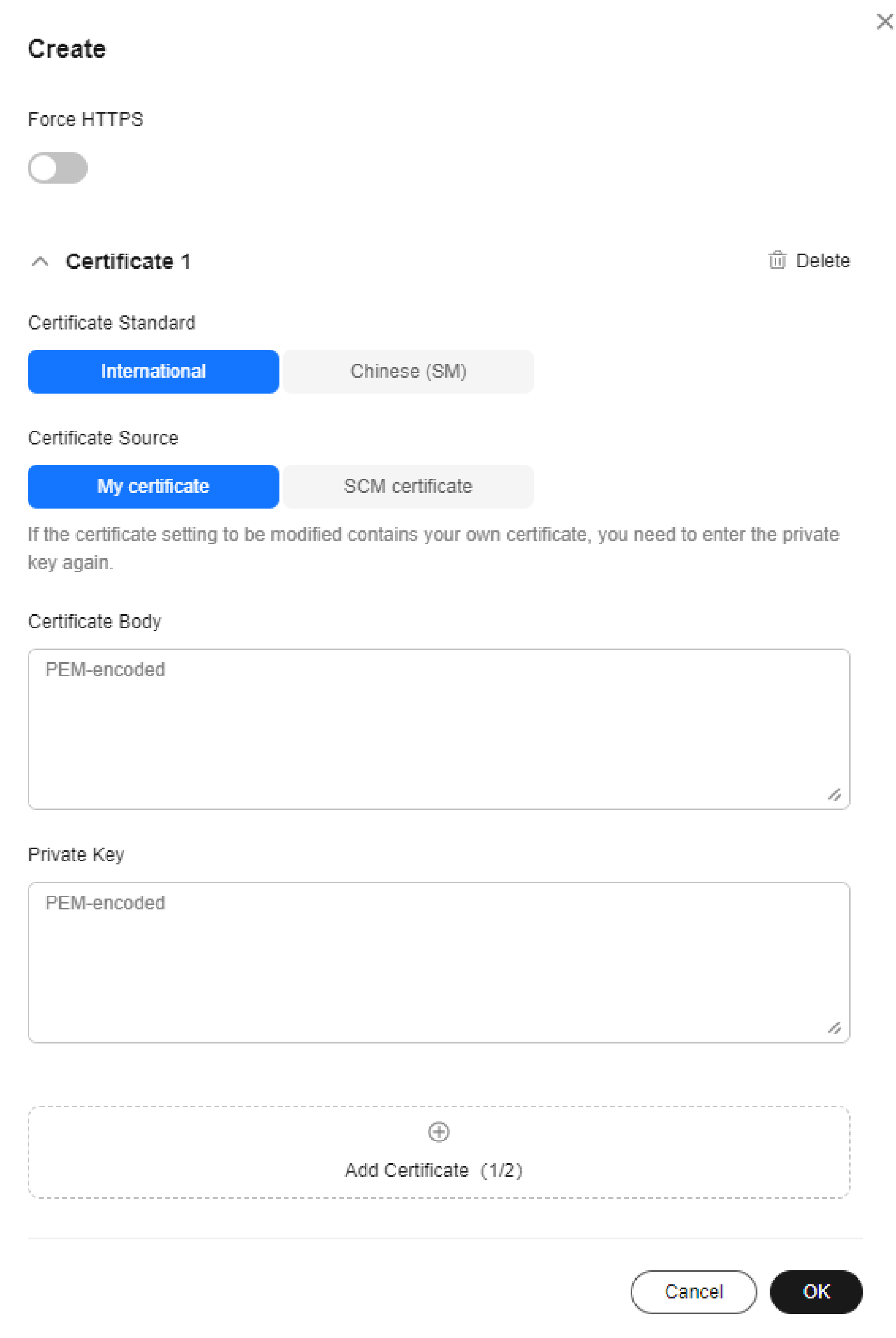
   Create

   Force HTTPS

6. Click **Add Certificate**. The settings of certificate 1 are displayed, as shown in **Figure 5-6**.

   Here is an example of adding a certificate of international standard. **Table 5-3** describes the parameters.

Figure 5-6 Creating certificate settings



Create

Force HTTPS

Certificate 1

Certificate Standard: International

Certificate Source: My certificate

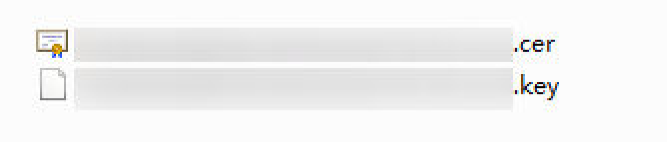
If the certificate setting to be modified contains your own certificate, you need to enter the private key again.

Certificate Body: PEM-encoded

Private Key: PEM-encoded

Table 5-3 Parameters

Parameter	Description
Certificate Standard	Select **International**.

Parameter	Description
Certificate Source	Select **My certificate**. The certificate must be obtained from an official channel.
International > **My certificate**	Open the obtained certificate file and private key file using a text tool, and copy the certificate body and private key content to the text boxes. Certificates issued by different organizations are different: ● If your certificate is issued by the root CA, the certificate is a complete one. Copy the certificate body. **Figure 5-7** HTTPS certificate  ● If your **certificate is issued by an intermediate CA**, the certificate file contains multiple certificates. You need to combine all the certificates into a single certificate.

7. Determine whether to enable **Force HTTPS**.

   If this option is enabled, all of your requests for the live video are converted to HTTPS requests.

8. Click **OK**.
9. Verify whether HTTPS secure acceleration has taken effect.

   Use an HTTPS streaming URL to play a video. If the playback is successful, HTTPS secure acceleration has taken effect.

   NOTE

   If your certificate is changed, you need to synchronize the new certificate to the HTTPS settings.

5.3 Pushing Streams and Streaming Content on a PC (for Cloud Stream Live)

This section describes how to push streams and stream content on a PC using the third-party software.

Prerequisites

- You have configured an ingest domain name and a streaming domain name on the Live console by referring to **Adding Domain Names**.

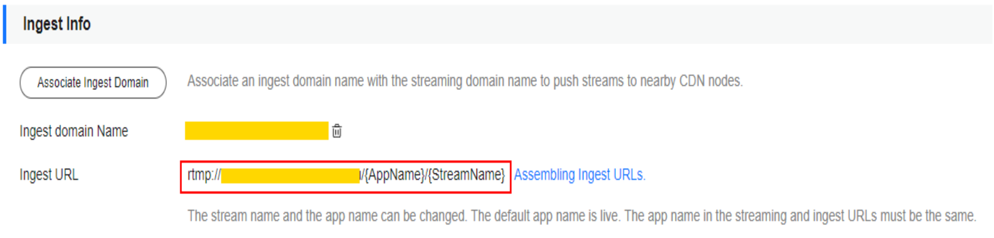
Pushing Streams

Step 1 Obtain an ingest URL.

1. Log in to the . In the navigation pane, choose **Domains**.
2. Click **Manage** in the **Operation** column of the desired ingest domain name. Obtain the ingest URL on the **Basic Info** page.

   See **Figure 5-8**. ***StreamName*** is user-defined. Example of ingest URL: **rtmp://livepush-test.huaweicloud.com/live/huawei09**.

Figure 5-8 Ingest URL



Ingest Info

Associate Ingest Domain — Associate an ingest domain name with the streaming domain name to push streams to nearby CDN nodes.

Ingest domain Name [redacted]

Ingest URL rtmp://[redacted]/{AppName}/{StreamName} Assembling Ingest URLs.

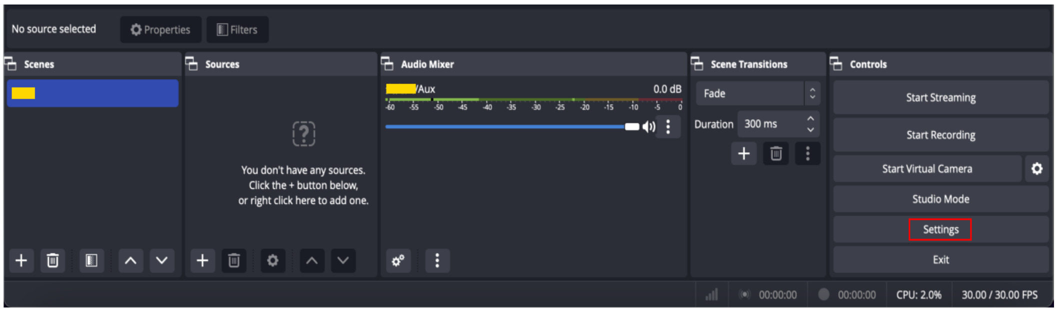
The stream name and the app name can be changed. The default app name is live. The app name in the streaming and ingest URLs must be the same.

NOTICE

The domain name in the preceding figure is only an example. Use your own ingest domain name.

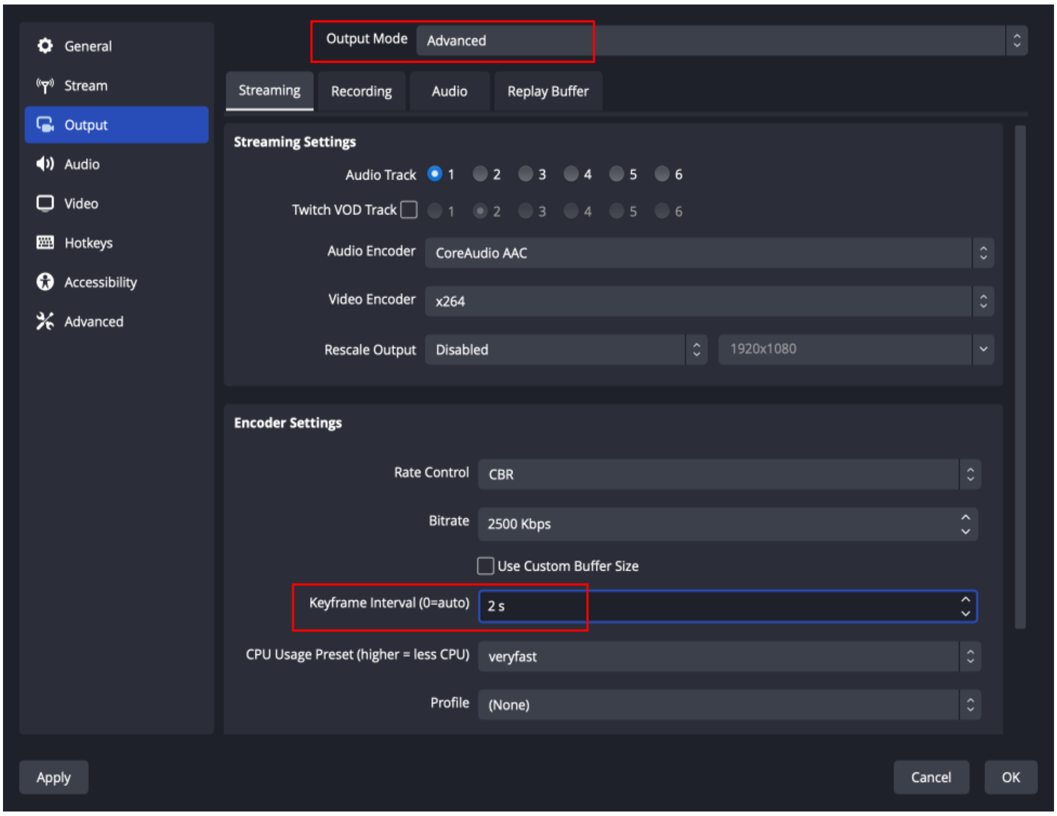
Step 2 Run OBS and click **Settings** in the lower right corner.

Figure 5-9 Settings



Step 3 On the left navigation pane, choose **Output**. Set **Output Mode** to **Advanced** and **Keyframe Interval** to **2**.

Figure 5-10 Output mode



Output Mode: Advanced

Streaming Settings

Audio Track: ● 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

Twitch VOD Track □ ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

Audio Encoder: CoreAudio AAC

Video Encoder: x264

Rescale Output: Disabled 1920x1080

Encoder Settings

Rate Control: CBR

Bitrate: 2500 Kbps

□ Use Custom Buffer Size

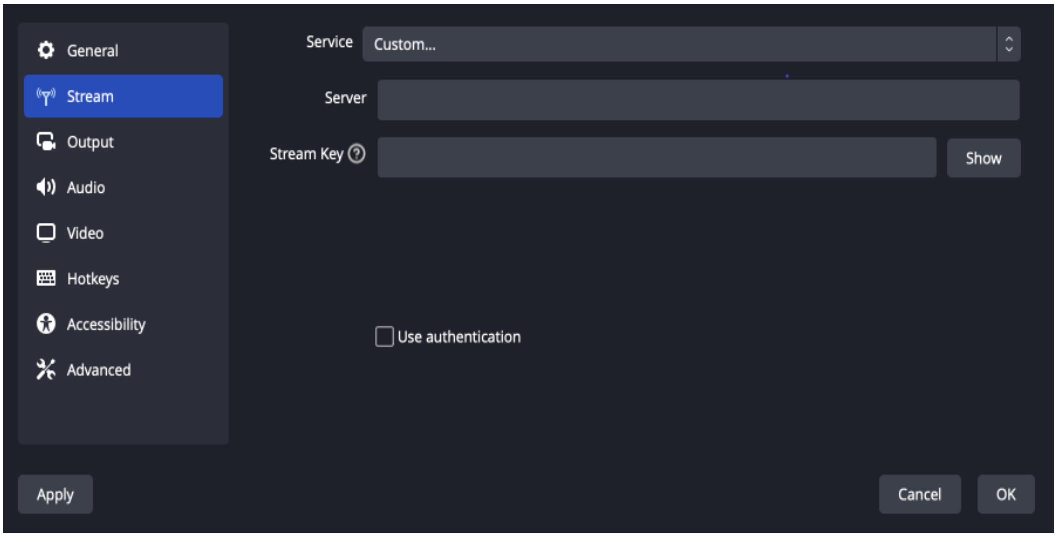
Keyframe Interval (0=auto): 2 s

CPU Usage Preset (higher = less CPU): veryfast

Profile: (None)

Step 4 In the navigation pane, choose **Stream** and enter the ingest URL obtained in 1.

Figure 5-11 Livestreaming settings



Service: Custom...

Server:

Stream Key:

□ Use authentication

An ingest URL consists of the following two parts:

- **URL**: Enter the part from the beginning of the ingest URL to the ***AppName***, for example, **rtmp://livepush-test.huaweicloud.com/live/**.
- **Stream Key**: Enter the part from the ***StreamName*** to the end of the ingest URL, for example, **huawei09**.

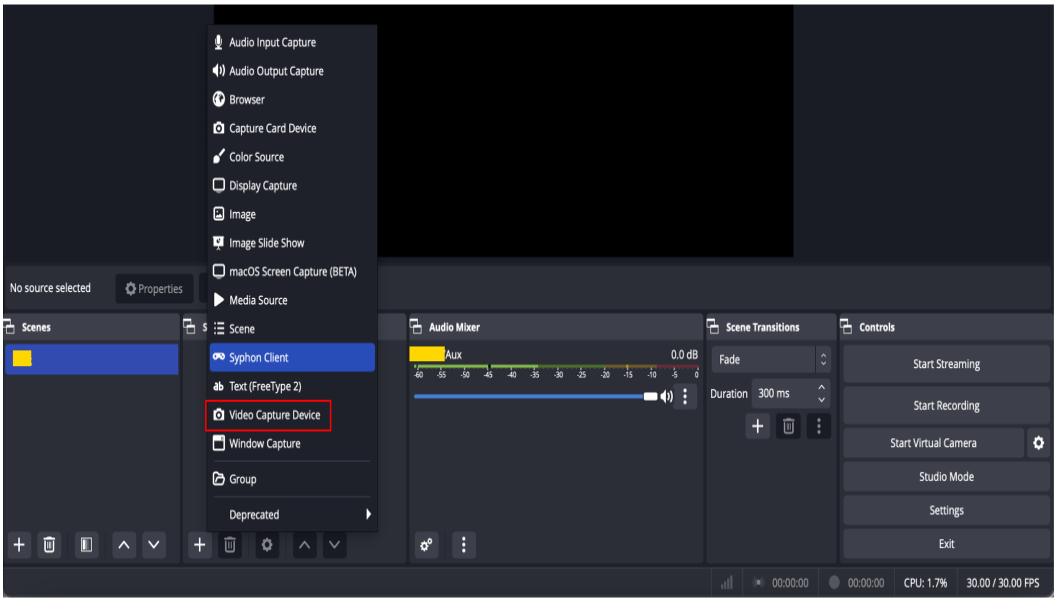
NOTE

The parameter names on the GUI may vary depending on the OBS version, but the rules for configuring the parameters are the same.

Step 5 Click **OK**.

Step 6 Right-click **+** in the lower left part of the **Sources** area to add a stream source.

Figure 5-12 Source settings



- **Media Source** indicates a local media file.
- **Video Capture Device** indicates a camera. If a camera is available on the PC, the camera is directly enabled.

Step 7 Click **Start Streaming** in the lower right corner.

----End

Streaming Content

Step 1 Obtain a streaming URL.

1. Log in to the . In the navigation pane, choose **Domains**.
2. Click **Manage** in the **Operation** column of the desired streaming domain name. Obtain the streaming URL on the **Basic Info** page.

   See **Figure 5-13**. ***StreamName*** is user-defined and must be the same as the value of ***StreamName*** in the ingest URL. Otherwise, the playback fails.

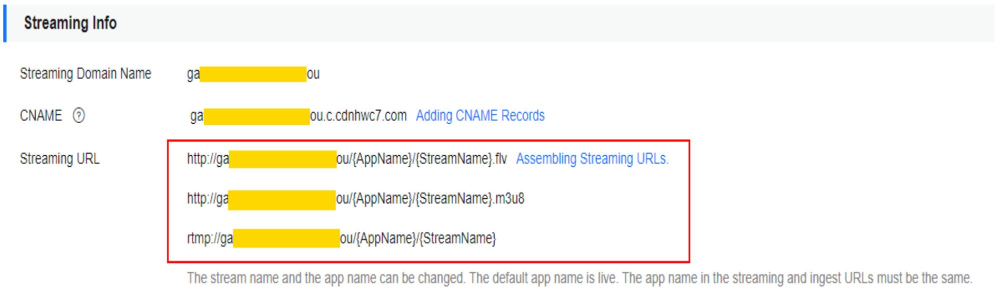
   For example, a streaming URL can be assembled in the following formats:

   – FLV: **http://exampletest.huaweicloud.com/live/huawei09.flv**

   – M3U8: **http://exampletest.huaweicloud.com/live/huawei09.m3u8**

   – RTMP: **rtmp://exampletest.huaweicloud.com/live/huawei09**

Figure 5-13 Streaming URL



Streaming Info

Streaming Domain Name ga[redacted]ou

CNAME ga[redacted]ou.c.cdnhwc7.com Adding CNAME Records

Streaming URL
http://ga[redacted]ou/{AppName}/{StreamName}.flv Assembling Streaming URLs.
http://ga[redacted]ou/{AppName}/{StreamName}.m3u8
rtmp://ga[redacted]ou/{AppName}/{StreamName}

The stream name and the app name can be changed. The default app name is live. The app name in the streaming and ingest URLs must be the same.

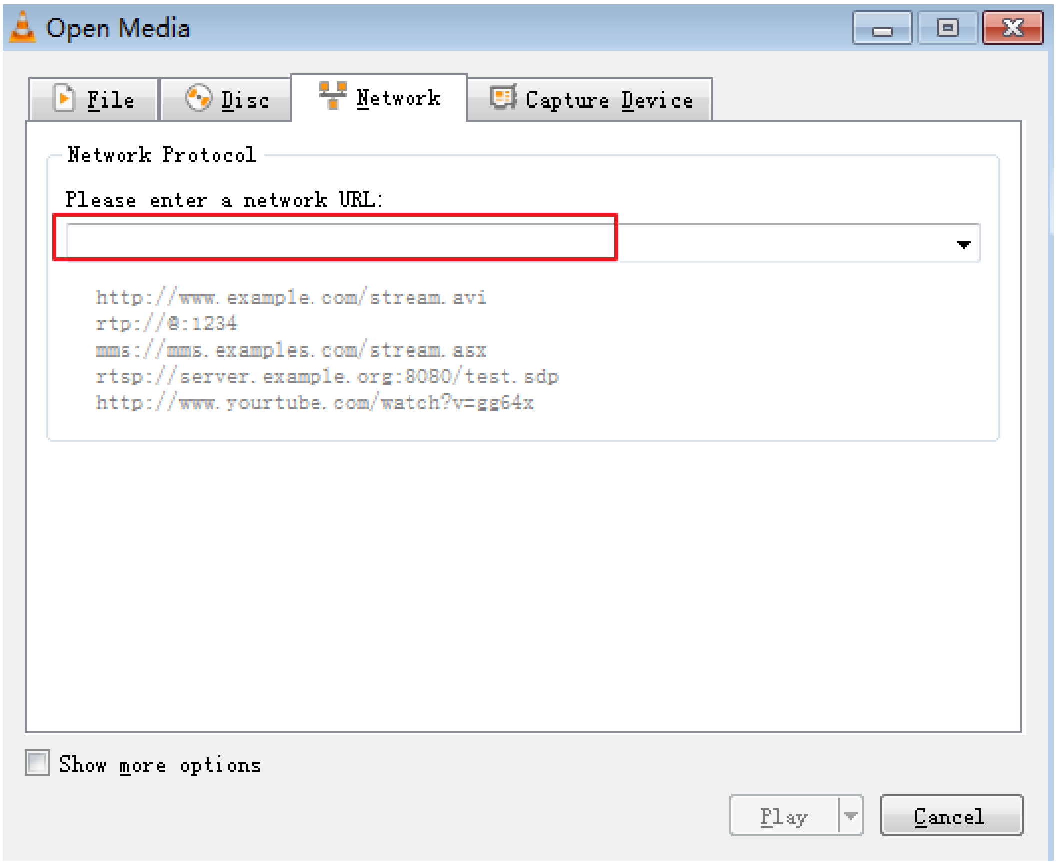
NOTICE

The domain name in the preceding figure is only an example. Use your own streaming domain name.

Step 2 Run VLC.

Step 3 On the menu bar, choose **Media** > **Open Multiple Files**.

Step 4 In the displayed dialog box, enter the streaming URL obtained in **step 1**. Click **Play**.



Network Protocol

Please enter a network URL:

```
http://www.example.com/stream.avi
rtp://@:1234
mms://mms.examples.com/stream.asx
rtsp://server.example.org:8080/test.sdp
http://www.yourtube.com/watch?v=gg64x
```

□ Show more options

----End

Helpful Links

If you use your own domain names for livestreaming, you can configure the following functions before using Live:

- **Recording a live video to OBS**
- **Snapshot capturing**
- **Transcoding**: used to transcode a livestream in different specifications and play the content using a transcoded streaming URL
- **Stream authentication**: used to protect live resources

5.4 Pushing Streams and Streaming Content on a PC (for Low Latency Live)

You can enter the generated ingest URL to the corresponding streaming software for stream push on LLL. Then, you can use the Huawei Cloud LLL online demo or API to play video on a web client.

Prerequisites

- You have installed a streaming tool (recommended: **Open Broadcaster Software**). If you have not installed it yet, download and install it.
- You have obtained the Huawei Cloud LLL online demo or called an API to play video on a web client.
- Contact Huawei Cloud technical support and to obtain the login address of the LLL console.

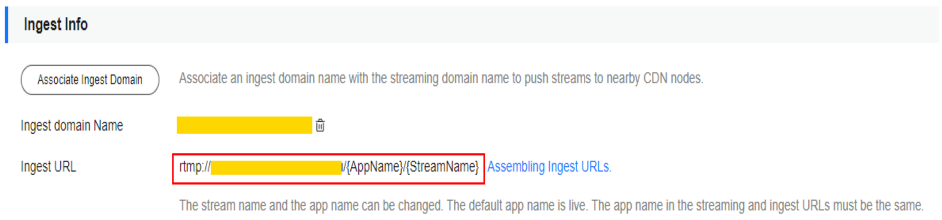
Pushing Streams

Open Broadcaster Software (OBS) is used as an example.

1. Obtain an ingest URL of LLL.
   a. Log in to the Live console. In the navigation pane, choose **Domains**.
   b. Click **Manage** in the **Operation** column of the desired ingest domain name. Obtain the ingest URL on the **Basic Info** page.

      See **Figure 5-14**. ***StreamName*** is user-defined. Example of ingest URL: **rtmp://livepush-test.huaweicloud.com/live/huawei09**.

Figure 5-14 Ingest URL



Ingest Info

Associate Ingest Domain

Associate an ingest domain name with the streaming domain name to push streams to nearby CDN nodes.

Ingest domain Name [redacted]

Ingest URL rtmp://[redacted]/{AppName}/{StreamName} Assembling Ingest URLs.

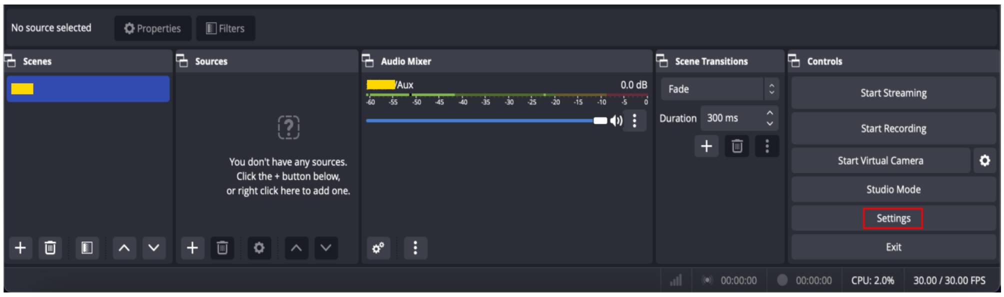
The stream name and the app name can be changed. The default app name is live. The app name in the streaming and ingest URLs must be the same.

NOTICE

The domain name in the preceding figure is only an example. Use your own ingest domain name.

2. Run OBS and click **Settings** in the lower right corner.

Figure 5-15 Settings



You don't have any sources.
Click the + button below,
or right click here to add one.

3. In the navigation pane, choose **Output**.

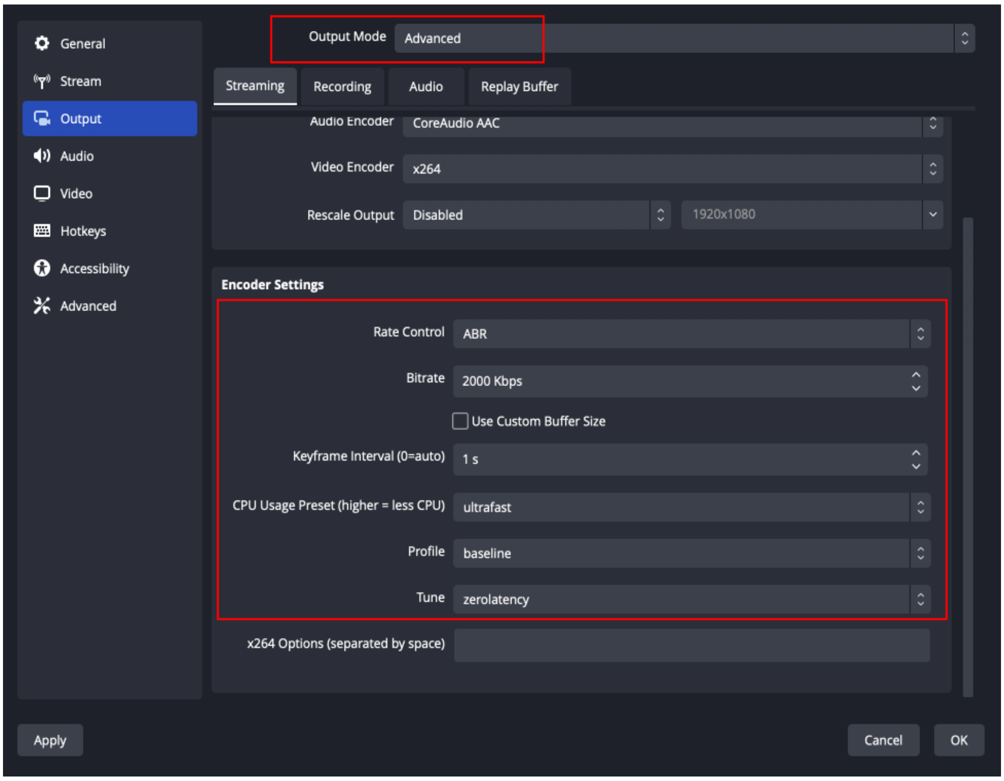
   Configure the following parameters as required and retain the default values for other parameters.

   – Set **Output Mode** to **Advanced**.
   – Set **Rate Control** to **ABR**.
   – Set **Bitrate** to **2000 Kbps**.
   – Set **Keyframe Interval** to **1**.
   – Set **CPU Usage Preset** to **ultrafast**.
   – Set **Profile** to **baseline**.
   – Set **Tune** to **zerolatency**.

   NOTE

   LLL does not push streams that contain B-frames. Therefore, you need to disable B-frames on OBS streaming devices.

Figure 5-16 Output mode



Output Mode: Advanced

Audio Encoder: CoreAudio AAC

Video Encoder: x264

Rescale Output: Disabled 1920x1080

Encoder Settings

Rate Control: ABR

Bitrate: 2000 Kbps

□ Use Custom Buffer Size

Keyframe Interval (0=auto): 1 s

CPU Usage Preset (higher = less CPU): ultrafast

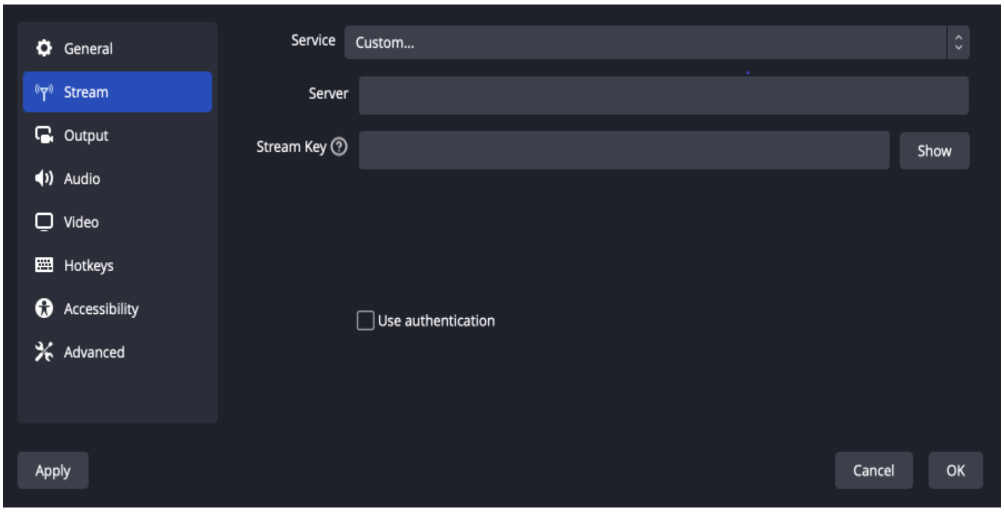
Profile: baseline

Tune: zerolatency

x264 Options (separated by space):

4. In the navigation pane, choose **Stream** and enter the ingest URL obtained in 1.

Figure 5-17 Livestreaming settings



Service: Custom...

Server:

Stream Key:

□ Use authentication

The ingest URL consists of the following two parts:

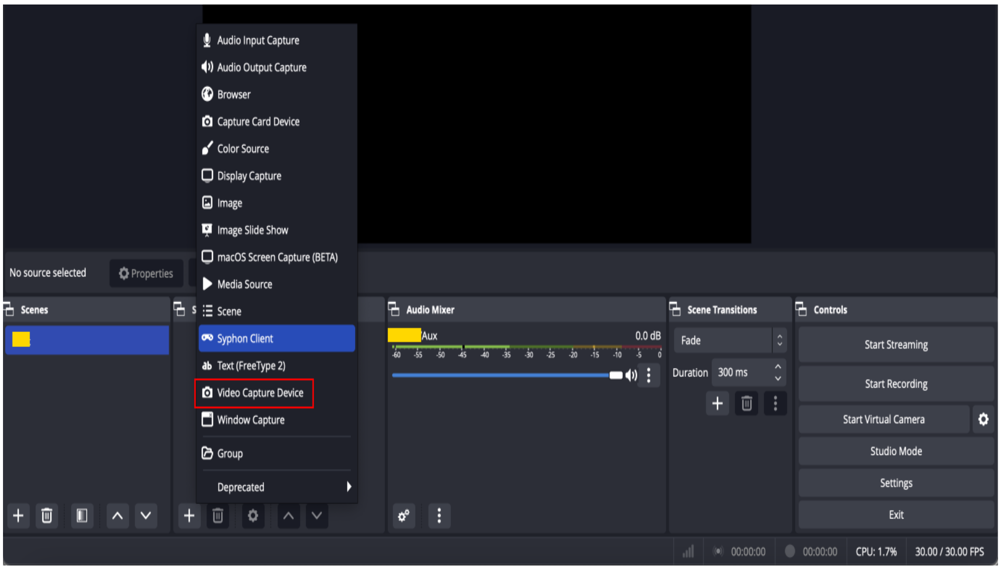
- **URL**: Enter the part from the beginning of the ingest URL to the ***AppName***, for example, **rtmp://livepush-test.huaweicloud.com/live/**.
- **Stream Key**: Enter the part from the ***StreamName*** to the end of the ingest URL, for example, **huawei01**.

NOTE

The parameter names on the GUI may vary depending on the OBS version, but the rules for configuring the parameters are the same.

5. Click **OK**.
6. Right-click **+** in the lower left part of the **Sources** area to add a stream source.

Figure 5-18 Source settings



- **Media Source** indicates a local media file.
- **Video Capture Device** indicates a camera. If a camera is available on the PC, the camera is directly enabled.

7. Click **Start Streaming** in the lower right corner.

Streaming Content (on a Web Client)

1. Obtain a streaming URL.
   a. Log in to the Live console. In the navigation pane, choose **Domains**.
   b. Click **Manage** in the **Operation** column of the desired streaming domain name. On the basic information page displayed, obtain the streaming URL.

      StreamName is user-defined and must be the same as the value of ***StreamName*** in the ingest URL. Otherwise, the playback fails.

      Example of an assembled streaming URL:

      webrtc://exampletest.huaweicloud.com/live/huawei09

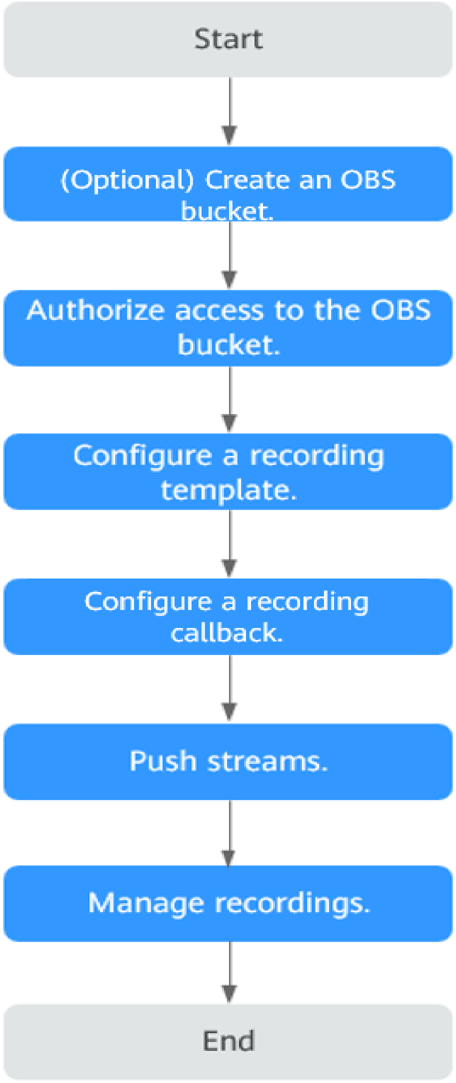
      exampletest.huaweicloud.com indicates the configured LLL domain name.
2. You can use the demo on the web client to check the livestream playback.

   Open the web test link of LLL and enter the streaming URL of LLL to try the playback.

5.5 Live Recording

The video recording process is the same for Cloud Stream Live and LLL, as shown in the following figure.

Live allows you to record a livestream and store the recordings in Object Storage Service (OBS), where you can download and share the recordings.


Start
(Optional) Create an OBS bucket.
Authorize access to the OBS bucket.
Configure a recording template.
Configure a recording callback.
Push streams.
Manage recordings.
End

1. **Create an OBS bucket for storing recordings**. For details about OBS pricing, see .
2. You need to **authorize Live** to store recording files in OBS buckets.
3. You can set the recording format and period. For details, see **Creating a Recording Template**.
4. **Configure a recording callback** if you want to know the recording status in real time.
5. Push streams.

6. **Manage recordings** on the OBS console, such as preview, download, and sharing.

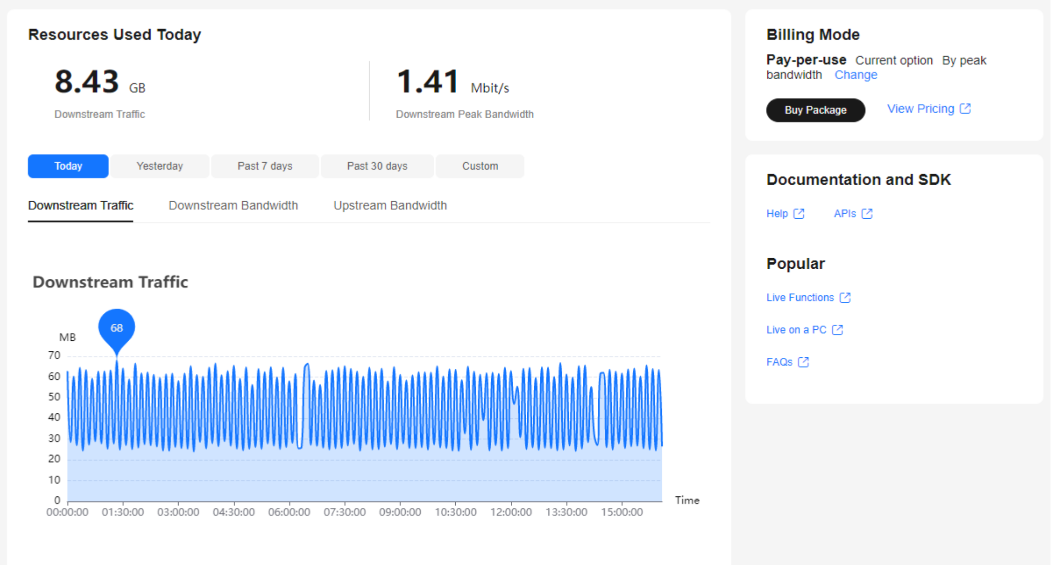
6 Functions of the Console

On the Live console, you can quickly configure basic functions such as the management of domain names and livestreams, transcoding, and recording. In addition, resource monitoring facilitates your real-time data analysis.

Dashboard

Log in to the **Live console**. The **Dashboard** page is displayed.

Figure 6-1 Dashboard



Resources Used Today

8.43 GB Downstream Traffic

1.41 Mbit/s Downstream Peak Bandwidth

Billing Mode

Pay-per-use Current option By peak bandwidth

On this page, you can check the following information. You can also click **Quick Links** in the upper right corner to read the documentation.

- **Today**
  - **Downstream Traffic**: total downstream traffic used by all streaming domain names on the current day
  - **Downstream Peak Bandwidth**: peak value of the downstream bandwidth used by all streaming domain names on the current day
- You can check the recent livestreaming resource usage trend.

  - **Downstream Traffic**: total downstream traffic used by all streaming domain names in a specific period
  - **Downstream Bandwidth**: total downstream bandwidth used by all streaming domain names in a specific period
  - **Upstream Bandwidth**: total upstream bandwidth used by the streaming device of a selected streaming domain name in a specific period

  NOTE

  You can point to the chart to view the specific value or scroll the mouse wheel to zoom in or out on the X-axis within a time range.

- **Billing Mode** displays the current CDN billing mode. You can click **Change** to change the CDN billing mode.

Functions

You can choose the functions in the navigation pane of the Live console.

Table 6-1 Functions of the console

Category	Function	Description
Streaming management	**Streaming**	You can manage ongoing streams and historical streams, such as disabling and resuming livestreams. This function is available only in **AP-Singapore** and **CN North-Beijing4**.
Domain name management	**Adding Domain Names**	You can add and manage your own domain names, configure CNAME records, referer validation, URL validation, and access control lists (ACLs) for domain names, and configure snapshot and transcoding templates.
Stream push	**Transcoding**	You can transcode livestreams into video streams with different resolutions and bitrates to meet a broad range of requirements.
	Creating a Recording Template	You can configure recording templates, record livestreams based on the templates, and store the recordings in OBS. This function is unavailable in AP-Bangkok.
	Snapshot Capturing	You can configure snapshot templates, capture snapshots from livestreams based on the templates, and store the snapshots in OBS. In **AP-Bangkok**, **submit a service ticket** to request for template review. The template takes effect only after it is approved.

Category	Function	Description
	Stream Status Notifications	You can configure callback URLs so that you can be notified of stream status in real time. In **AP-Bangkok**, **submit a service ticket** to request for template review. The template takes effect only after it is approved.
	Stream Authentication	You can configure URL validation and ACLs to identify and filter out malicious streaming requests.
Playback	**Configuring Stream Delay**	You can configure the delay for RTMP and HTTP-FLV streaming.
	Configuring Origin Pull	You can pull live content from your own origin server to Huawei Cloud Live origin server for accelerated delivery.
	Configuration Method	You can enable HTTPS secure acceleration for streaming domain names to encrypt your live content during transmission.
	Overview	You can configure referer validation, URL validation, and ACLs to identify and filter out malicious visitors.
Usage statistics	**Usage Statistics**	You can check the downstream bandwidth/traffic of all streaming domain names, and the total transcoding duration, maximum number of concurrent recording streams, and number of snapshots of all ingest domain names.
Service monitoring	**Service Monitoring**	You can check data of a streaming domain name, such as the downstream bandwidth/traffic, stream playback profile, status codes returned in the response, and the number of online viewers of the corresponding livestream. You can also check data of the ingest domain name, such as the upstream bandwidth/traffic, total number of streams, pushed stream details, and frame rate/bitrate of a pushed stream.
Log management	**Offline Log Download**	You can check logs about requests to a streaming domain name and query and download log files over the past 90 days.
Tools	**Signed URL Generation Tool**	You can quickly generate signed URLs for streaming and ingest domain names.

7 Prerequisites

Before using Live, you need to perform the operations in this section.

Real-Name Authentication

Individual or enterprise users must complete real-name authentication.

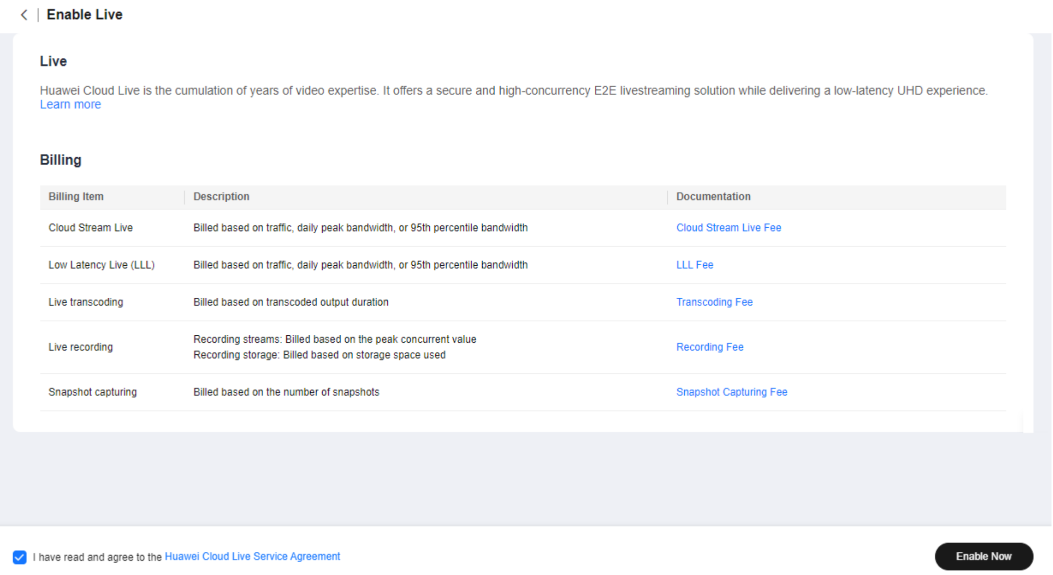
Account Balance

By default, Live uses pay-per-use billing. The generated service fees will be directly deducted from your account balance. Ensure that your account is available and has sufficient balance.

Risk Warning on the First Service Enabling

If you purchase Live for the first time, the page shown in **Figure 7-1** will be displayed. You need to check the details of each billing item and read the *Huawei Cloud Live Service Agreement* carefully before enabling Live.

Figure 7-1 Enabling Live



< | Enable Live

Live

Huawei Cloud Live is the cumulation of years of video expertise. It offers a secure and high-concurrency E2E livestreaming solution while delivering a low-latency UHD experience. Learn more

Billing

Billing Item	Description	Documentation
Cloud Stream Live	Billed based on traffic, daily peak bandwidth, or 95th percentile bandwidth	Cloud Stream Live Fee
Low Latency Live (LLL)	Billed based on traffic, daily peak bandwidth, or 95th percentile bandwidth	LLL Fee
Live transcoding	Billed based on transcoded output duration	Transcoding Fee
Live recording	Recording streams: Billed based on the peak concurrent value Recording storage: Billed based on storage space used	Recording Fee
Snapshot capturing	Billed based on the number of snapshots	Snapshot Capturing Fee

☑ I have read and agree to the Huawei Cloud Live Service Agreement

Enabling Live

For details, see **Getting Started**.

8 Permissions Management

8.1 Creating a User and Assigning Live Permissions

This section describes how to use **IAM** to implement refined permissions management for your Live resources. With IAM, you can:

- Create IAM users for employees from different departments of your enterprise. In this way, each IAM user has a unique security credential to use Live resources.
- Assign 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 Live resources.

If your Huawei Cloud account does not require individual IAM users, skip this section.

This section describes the procedure for assigning permissions. For details, see **Figure 8-1**.

Notes

- **Submit a service ticket** to apply for permissions management in either of the following cases:
  - You had created domain names in the AP-Singapore region before March 1, 2022.
  - You had created domain names in the CN North-Beijing4 region before March 16, 2022.

  After **permissions management** is enabled, unauthorized **IAM users** cannot call Live APIs. Ensure that IAM users have been assigned the Live permissions.
- If you use a custom policy but do not use the system-defined permissions **Live FullAccess** and **Live ReadOnlyAccess**, you need to add the operation permission **live:tenant:getTenantInformation** before accessing the Live console.
- After assigning an IAM user the **Live FullAccess** permission, you need to assign the user the following Cloud Eye permissions to monitor metrics of Live:

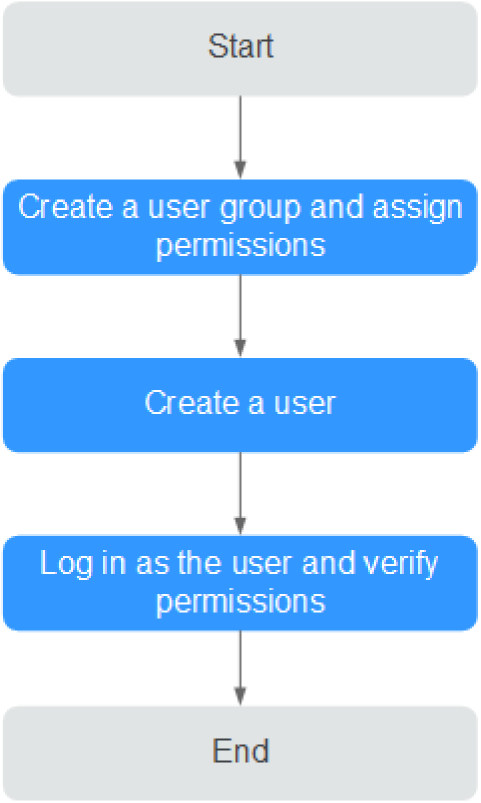
- **CES ReadOnlyAccess**: On the Cloud Eye console, choose **Cloud Service Monitoring** > **Live** to view resource monitoring metrics of Live.
- **CES FullAccess**: On the Cloud Eye console, choose **Cloud Service Monitoring** > **Live** to view resource monitoring metrics of Live and perform operations.

Prerequisites

Learn about the **system-defined permissions on Live** that can be assigned to a user group and assign the permissions as required.

Process Flow

Figure 8-1 Process for assigning read-only permissions on Live


Start
Create a user group and assign permissions
Create a user
Log in as the user and verify permissions
End

1. **Creating a user group and assigning permissions**

   Create a user group on the IAM console and assign it the **Live ReadOnlyAccess** policy.

2. **Creating a user and adding them to the user group**

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

3. **Logging in as the user** and verifying permissions

   Log in to the console as the created user, and select an authorized region to verify permissions:

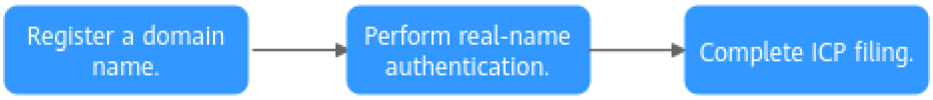
   Choose **Live** in **Media Services** under **All Services**. On the Live console, choose **Domains** in the navigation pane to add a domain name. If a message is displayed indicating insufficient permissions for performing the operation, the **Live ReadOnlyAccess** policy has taken effect.

9 Domain Name Management

9.1 Domain Name Admission Standards

Before using your domain name on Huawei Cloud Live, you can read this section to understand the access conditions and restrictions of acceleration domain names to avoid losses caused by rule violations.

Admission Process



1. Register a domain name: If you do not have a domain name,

   NOTE

   A top-level domain name cannot be used as an ingest domain or streaming domain. If your domain name is **example.com**, you can use second-level domain names, for example, **test-push.example.com** as the ingest domain and **test-play.example.com** as the streaming domain.

2. Perform real-name authentication: You can log in to the **Huawei Cloud official website** and complete real-name authentication for individuals or enterprises.

   NOTE

   If you are a user of Huawei Cloud (International) or Huawei Cloud (Europe), you need to complete real-name authentication when you:

   - Purchase and use cloud services in Huawei Cloud regions in the Chinese mainland. In this case, real-name authentication is required by the laws and regulations of the Chinese mainland.
   - Plan to use Live in Huawei Cloud regions in the Chinese mainland.

3. Complete ICP filing: If you want to perform livestreaming acceleration in Huawei Cloud regions in or outside the Chinese mainland, the domain names must complete ICP filing in advance as required by the Ministry of Industry and Information Technology (MIIT).

Quantity Limit

By default, you can add up to 64 domain names in your account. If you have additional requirements, **submit a service ticket**.

Content Moderation

Live does not allow accessing websites that violate related laws and regulations, including but not limited to:

- Websites that contain pornographic content or content related to gambling, illegal drugs, frauds, or infringement
- Gaming websites that run on illegal private servers
- Websites that provide pirated games/software/videos
- P2P lending websites
- Unofficial lottery websites
- Unlicensed hospital and pharmaceutical websites
- Inaccessible websites or websites that do not contain any substantial information

NOTE

- If the use of your domain name violates related laws and regulations, you shall bear the related risks.
- If any pornographic content or content related to gambling, illegal drugs, or frauds is found on your domain name, the domain name and other domain names that use the same origin server will be deleted from Live and can no longer access Live. Acceleration domain name quota of the account will be reduced to 0.

Domain Name Rules

See **Table 9-1**.

Table 9-1 Domain name rules

Domain Name Status	Rule
A domain name that has no access traffic for more than 90 days (the domain name is either working or malfunctioning)	The domain name will be automatically disabled and the records related to the domain name will be saved. If you want to continue using the domain name, enable it again.
A domain name that has been disabled for more than 90 days (the domain name may not have been approved)	The records related to the domain name will be automatically deleted. If you want to continue using the domain name, add it again.

9.2 Adding Domain Names

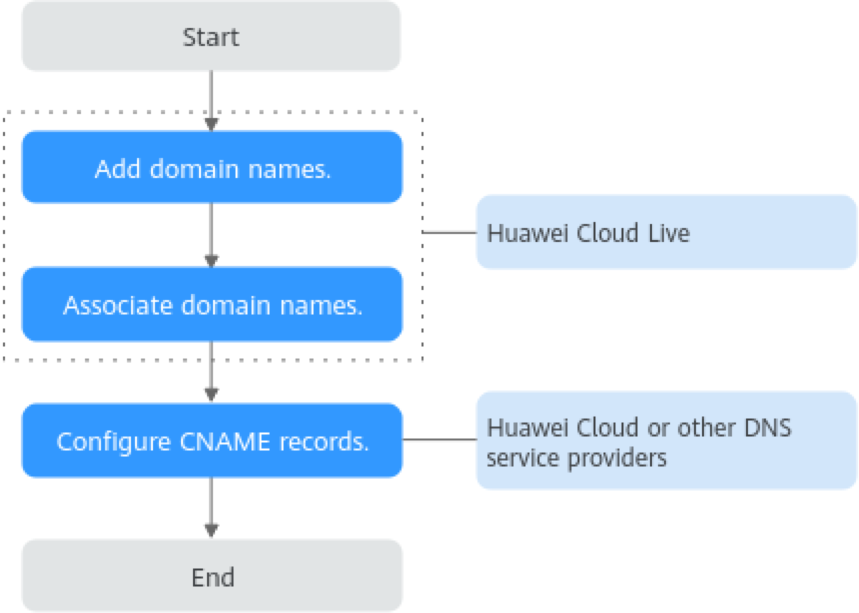
Before using Live, you must add ingest domain names and streaming domain names to Live.

Before connecting your domain name to Huawei Cloud Live, you need to understand the access conditions and restrictions of acceleration domain names to avoid losses caused by rule violations. For details, see **Domain Name Admission Standards**.

Domain Name Admission Process

Figure 9-1 shows the process of using your own domain name for livestreaming acceleration.

Figure 9-1 Domain name admission process



1. **Add an ingest domain name and a streaming domain name (both licensed) to Live**.
2. **Associate the ingest domain name with the streaming domain name**.
3. **Configure CNAME records** at your domain names' DNS provider so that the CNAME records allocated to Live point to the domain names.

Prerequisites

- You have registered with Huawei Cloud and completed real-name authentication.

> **NOTE**
>
> If you are a user of Huawei Cloud (International) or Huawei Cloud (Europe), you need to complete real-name authentication when you:
>
> - Purchase and use cloud services in Huawei Cloud regions in the Chinese mainland. In this case, real-name authentication is required by the laws and regulations of the Chinese mainland.
> - Plan to use Live in Huawei Cloud regions in the Chinese mainland.

- Domain names for Live are available. Live requires an ingest domain name and a streaming domain name, and the two domain names must be different.

> **NOTE**
>
> If you want to perform livestreaming acceleration in Huawei Cloud regions in or outside the Chinese mainland, the domain names must complete ICP filing in advance as required by the Ministry of Industry and Information Technology (MIIT).

Notes

- An area needs to be specified for stream push, and the streaming domain name needs to be associated with an ingest domain name. In this way, a streaming domain name can be used to watch livestreaming in the area where the ingest domain name is located. That is, a streaming domain name cannot be used to watch livestreaming in and outside China at the same time.
- The price of livestreaming outside China is different from that in China. For details, see **Pricing Details**.
- If the streaming URL is not used in the selected acceleration area, the playback quality may be compromised.
- If the **Service Area** of the streaming domain name is **Chinese mainland** or **Global**, and the origin server of the ingest domain name is in the Chinese mainland, the domain names must be licensed in the Chinese mainland.
- If you add, modify, or delete a domain name, the change will be displayed in My Resources within 24 hours. Please check the data later.

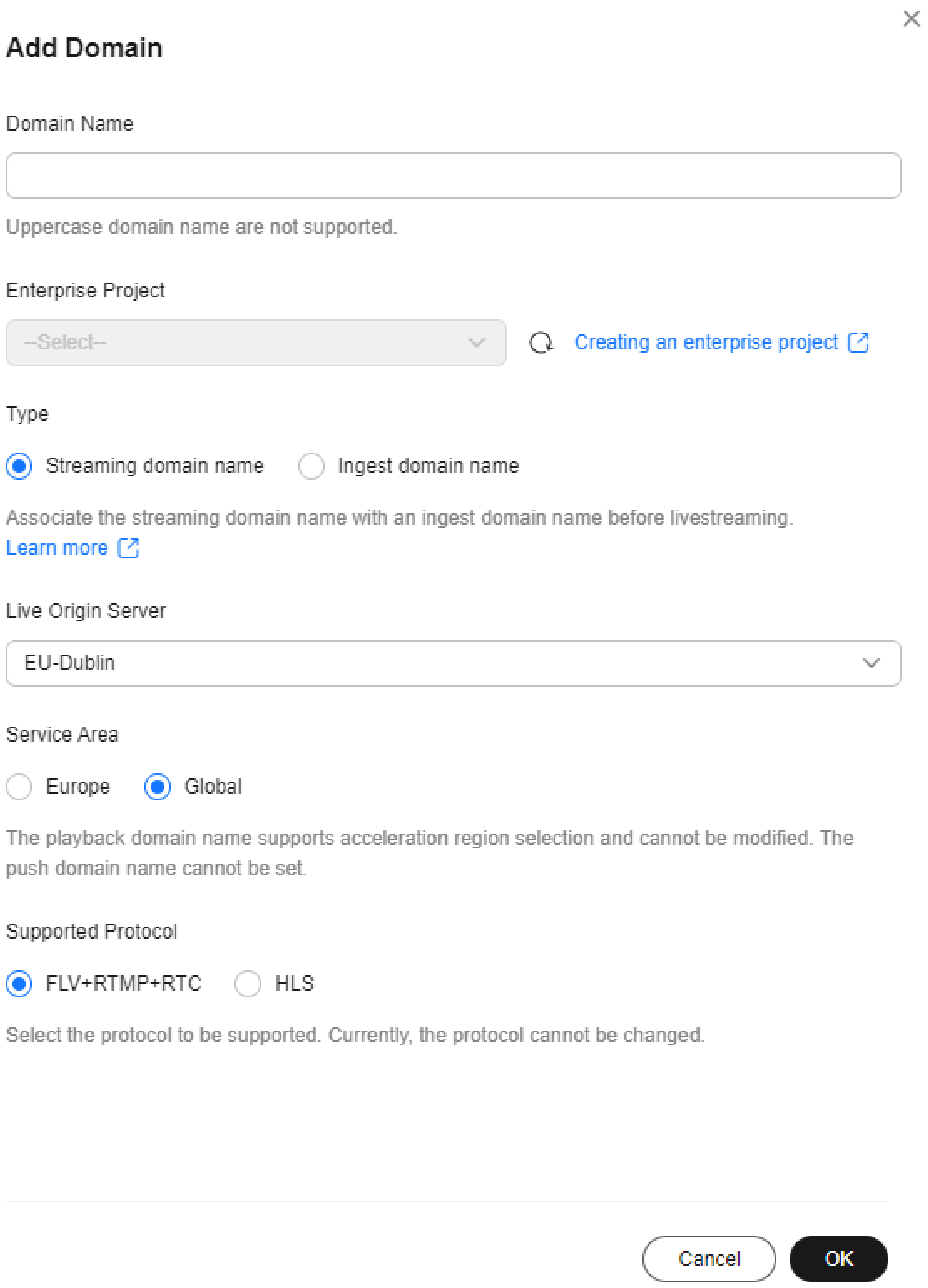
Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Add Domain**. On the displayed page, enter a streaming or ingest domain name.

Figure 9-2 Adding a domain name



Add Domain

Domain Name

Uppercase domain name are not supported.

Enterprise Project

--Select--

Creating an enterprise project

Type

● Streaming domain name ○ Ingest domain name

Associate the streaming domain name with an ingest domain name before livestreaming.
Learn more

Live Origin Server

EU-Dublin

Service Area

○ Europe ● Global

The playback domain name supports acceleration region selection and cannot be modified. The push domain name cannot be set.

Supported Protocol

● FLV+RTMP+RTC ○ HLS

Select the protocol to be supported. Currently, the protocol cannot be changed.

Table 9-2 Domain name parameters

Parameter	Description
Domain Name	Enter a second-level ingest domain name or streaming domain name, for example, test-push.example.com. **NOTE** ● The domain name can contain a maximum of 64 characters, which cannot contain uppercase letters. ● An ingest domain name must be different from a streaming domain name. Wildcard domains are not allowed. ● By default, you can add up to 64 domain names in your account. To add more domain names, **submit a service ticket**.
Enterprise Project	Add domain names to enterprise projects for unified management. On the **Create Enterprise Project** page, **create an enterprise project** (whose name is **default** by default) and **add the user group to the enterprise project**. By doing so, users in this user group obtain the permissions on the domain names in the enterprise project. **NOTE** Only an enterprise account can configure enterprise projects.
Type	If you enter an ingest domain name for **Domain Name**, then select **Ingest domain name** for **Type**. The domain name type cannot be changed once configured.
Live Origin Server	Area where the Live origin server is located. For details, see How Do I Select a Live Origin Server and Acceleration Area? The Live origin server cannot be changed once configured. Select the nearest origin server. Currently, Live origin servers are deployed in the following regions: ● CN North-Beijing4 of Huawei Cloud (Chinese Mainland): CN North-Beijing4 and AP-Singapore. ● Singapore of Huawei Cloud (International): AP-Singapore, LA-Sao Paulo1, and CN North-Beijing4. ● Dublin of Huawei Cloud (Europe): EU-Dublin. **NOTE** ● The origin server of the ingest domain name must be in the region where the streamer is. Streamers cannot push streams across regions. For example, if a streamer needs to livestream in both the Chinese mainland and Malaysia, two sets of streaming and ingest domain names need to be configured. The origin servers of each set of domain names are located in the Chinese mainland and Singapore, respectively. ● The origin servers of the ingest and streaming domain names to be associated must be in the same region. ● The OBS buckets that you use for storing live video recordings and snapshots must be in the same region as the Live origin server.

Parameter	Description
Service Area	Area where streaming domain names can be accelerated. For details, see How Do I Select a Live Origin Server and Acceleration Area? This parameter is valid only for streaming domain names and cannot be changed once configured. If the video is not played in the selected acceleration area, the livestreaming quality may be compromised. Select an acceleration area that fits your needs. Options: ● **Europe** Select this option when the audience is in Europe. ● **Global** Select this option when the audience is not in Europe. If you select **Global** as the acceleration area, when you or your end users use the domain name, the configuration data of the domain name, including audio and video data, may be transferred across borders in the following scenarios: ● Audio and video data is transferred across borders from Ireland to the country or region where your end users are. ● The configuration data of the domain name is transferred from Ireland to Singapore. **NOTICE** If the **Service Area** you select involves cross-border data transfer, you shall be responsible for such transfer. For details, see section 2.3 "Processing Your Content Data" of **Live Service Agreement**.
Supported Protocol	Streaming protocols supported by a streaming domain name. ● This parameter is valid only for streaming domain names. ● The value defaults to **FLV+RTMP+RTC** and cannot be changed once specified. Options: ● **FLV+RTMP+RTC**: The streaming domain name can use HTTP-FLV, RTMP, and WebRTC to play Cloud Live content. ● **HLS**: The streaming domain name can use HLS to play Cloud Live content.

Step 4 Click **OK**.

A domain name whose **Status** is **Configuring** is displayed in the domain name list. If **Status** becomes **Normal** in 3 to 5 minutes, the domain name has been added.

Step 5 After adding the streaming domain name, you need to associate the streaming domain name with the ingest domain name before using Live. The associated ingest domain name and streaming domain name must belong to the same Live origin server. For details, see **Associating Domain Names**.

Step 6 **Configure CNAME records** at your domain names' DNS provider so that the CNAME records allocated to CDN point to the domain names. Once the configuration takes effect, livestreaming acceleration is automatically enabled for the domain names.

----End

Follow-up Operations

After domain names are added, you can configure the following settings for the ingest and streaming domain names.

- Configure a recording, transcoding, or snapshot template for your ingest domain name. For details, see **Creating a Recording Template**, **Transcoding**, and **Snapshot Capturing**.
- Configure playback authentication for your streaming domain name. For details, see **Overview**.

9.3 Associating Domain Names

After an ingest domain name and streaming domain name are added, you must associate them so that they can take effect.

Notes

You can associate only one ingest domain name with a streaming domain name.

Prerequisites

You have added an ingest domain name and streaming domain name by referring to **Procedure**.

Procedure

Step 1 Log in to the **Live console**.

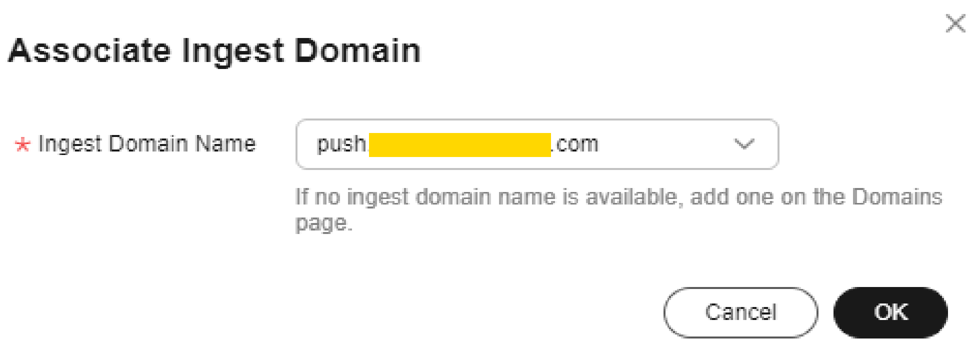
Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Manage** in the **Operation** column of the desired streaming domain name.

The **Basic Info** page is displayed.

Step 4 In the **Ingest Info** area, click **Associate Ingest Domain** and select the added ingest domain name.

Figure 9-3 Associating domain names



Associate Ingest Domain

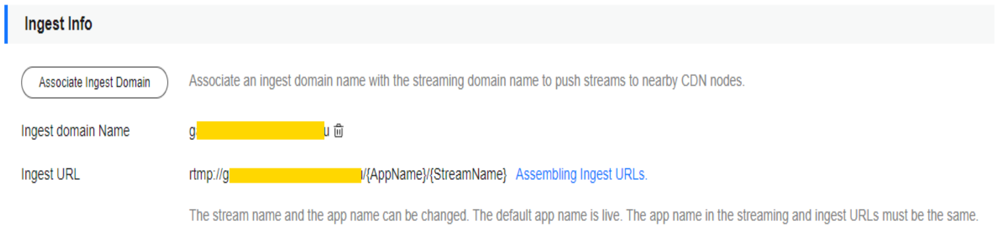
* Ingest Domain Name: push[redacted].com

If no ingest domain name is available, add one on the Domains page.

Step 5 Click **OK**.

Information about stream push is displayed.

Figure 9-4 Ingest Info



Ingest Info

Associate an ingest domain name with the streaming domain name to push streams to nearby CDN nodes.

Ingest domain Name: g[redacted]u

Ingest URL: rtmp://g[redacted]/{AppName}/{StreamName} Assembling Ingest URLs.

The stream name and the app name can be changed. The default app name is live. The app name in the streaming and ingest URLs must be the same.

----End

9.4 Configuring CNAME Records

After a domain name is added, a CNAME record is automatically assigned to the domain name. You need to configure the CNAME record at your domain names' DNS provider. Acceleration is enabled once the configuration takes effect.

Notes

- If the domain name you added is on Huawei Cloud, configure the CNAME record following the **Procedure**. If the domain name you added is not on Huawei Cloud, configure the CNAME record following the guidance provided by your domain names' DNS provider.
- Configure CNAME records for the ingest domain name and streaming domain name separately.

Prerequisites

The ingest domain name and streaming domain name have been **added** and **associated**.

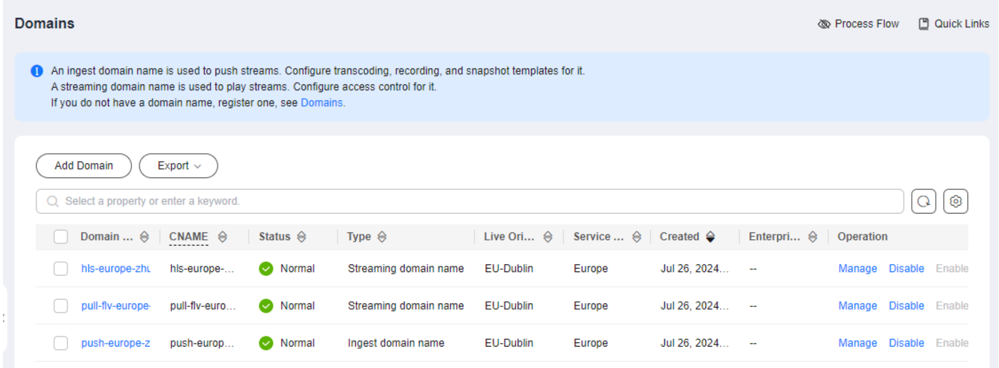
Procedure

The following uses a streaming domain name as an example. The procedure for configuring the CNAME record for an ingest domain name is the same.

Step 1 Obtain the CNAME record.

1. Log in to the **Live console**.
2. In the navigation pane on the left, choose **Domains**.
3. Obtain the corresponding CNAME record in the **CNAME** column.

Figure 9-5 Obtaining the CNAME record



An ingest domain name is used to push streams. Configure transcoding, recording, and snapshot templates for it.
A streaming domain name is used to play streams. Configure access control for it.
If you do not have a domain name, register one, see Domains.

Select a property or enter a keyword.

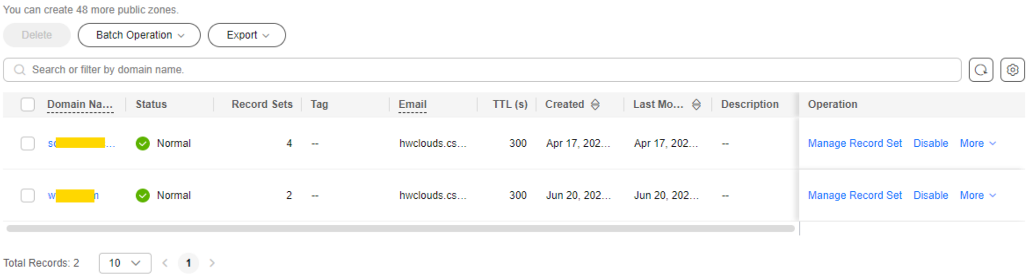
□	Domain ...	CNAME	Status	Type	Live Ori...	Service ...	Created	Enterpri...	Operation
□	hls-europe-zhu	hls-europe-...	Normal	Streaming domain name	EU-Dublin	Europe	Jul 26, 2024...	--	Manage Disable Enable
□	pull-flv-europe-	pull-flv-euro...	Normal	Streaming domain name	EU-Dublin	Europe	Jul 26, 2024...	--	Manage Disable Enable
□	push-europe-z	push-europ...	Normal	Ingest domain name	EU-Dublin	Europe	Jul 26, 2024...	--	Manage Disable Enable

Step 2 Log in to the **Domain Name Service (DNS)** console.

Step 3 In the navigation pane on the left, choose **Public Zones**.

Step 4 Click the target domain name in the **Domain Name** column, as shown in **Figure 9-6**.

Figure 9-6 Domain name list



You can create 48 more public zones.

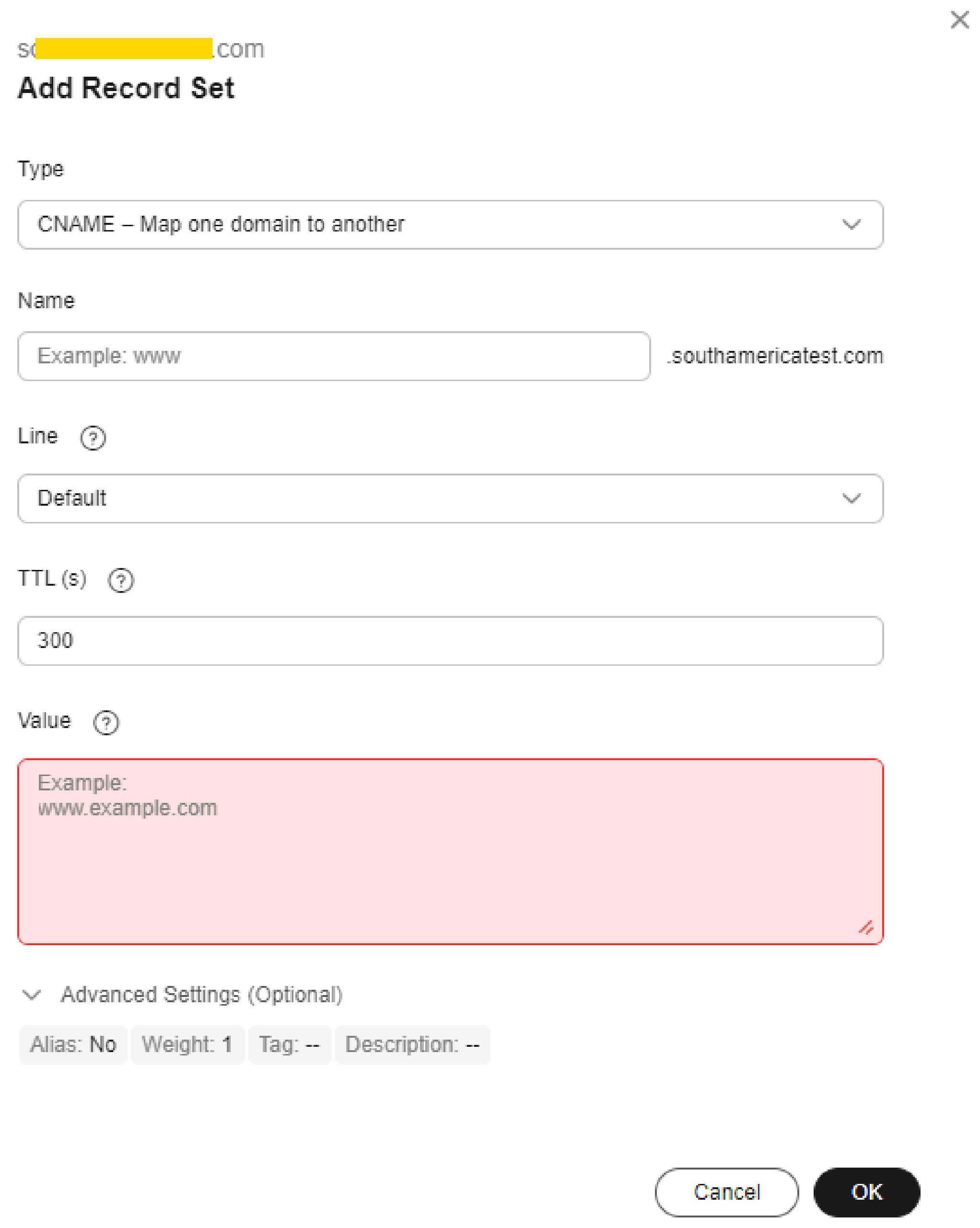
Search or filter by domain name.

□	Domain Na...	Status	Record Sets	Tag	Email	TTL (s)	Created	Last Mo...	Description	Operation
□	[redacted]	Normal	4	--	hwclouds.cs...	300	Apr 17, 202...	Apr 17, 202...	--	Manage Record Set Disable More
□	[redacted]	Normal	2	--	hwclouds.cs...	300	Jun 20, 202...	Jun 20, 202...	--	Manage Record Set Disable More

Total Records: 2 10 < 1 >

Step 5 Click **Add Record Set** in the upper right corner.

Figure 9-7 Adding a record set



sc[redacted].com

Add Record Set

Type: CNAME – Map one domain to another

Name: Example: www .southamericatest.com

Line: Default

TTL (s): 300

Value: Example: www.example.com

Advanced Settings (Optional)

Alias: No | Weight: 1 | Tag: -- | Description: --

Configure the parameters by referring to **Table 9-3**.

Table 9-3 Parameters

Parameter	Description
Type	Type of the record set. Select **CNAME – Map one domain to another** here.

Parameter	Description
Name	Enter the second-level domain name. You do not need to enter the suffix. For example, if the streaming domain name is **play-test.example.com**, enter **play-test**.
Line	Used when the DNS server is resolving a domain name. It returns the IP address of the server according to the visitor source. For details, see **Resolution Lines**. This parameter is available only for public domain names. Select **Default**.
TTL (s)	Cache duration of the record set on a local DNS server, in seconds. The smaller the value is, the quicker the record takes effective. The default value is 300 seconds. You can retain the default value.
Value	Domain name to be pointed to, that is, the CNAME record obtained in step 1 of this section. For example, if the streaming domain name is **play-test.example.com**, enter **play-test.example.com.c.cdnhwc3.com**.
Alias	Whether to associate the record set with a cloud resource. ● Enabled: The record set will be associated with a cloud resource. ● Disabled: The record set will not be associated with a cloud resource. Toggle off the switch, that is, disable this function.
Weight	(Optional) Weight of a record set. The value ranges from **0** to **1000** and defaults to **1**. This parameter is available only for public domain names. If a resolution line in a zone contains multiple record sets of the same type, you can **configure weighted routing** for each record set. Set this parameter to **1**.
Tag	(Optional) Identifier of a record set. Each tag contains a key and a value. You can add up to 10 tags to a record set. For details about how to name a key and a value, see **Adding a CNAME Record Set**. Examples: ● example_key1 ● example_value1
Description	(Optional) Describes a domain name. The description can contain a maximum of 255 characters.

Step 6 Click **OK**.

The record set you added is displayed in the list. If the status of the record set is **Normal**, the record set has been added.

Step 7 Perform 1 to 6 to configure the CNAME record for the ingest domain name.

----End

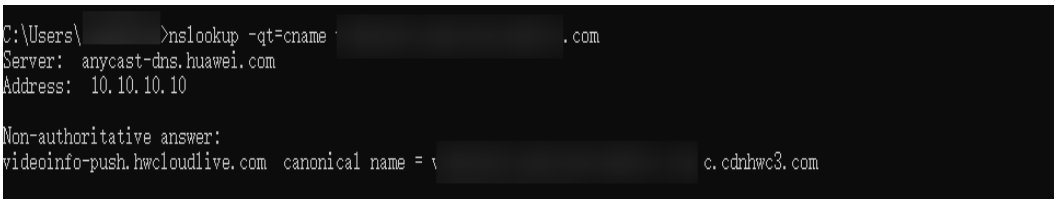
Checking Whether the CNAME Record Has Taken Effect

Open the command line interface that comes with Windows and run the following command:

```
nslookup -qt=cname Acceleration domain name
```

If the CNAME record is displayed, the CNAME record has taken effect. A typical command output is shown in **Figure 9-8**.

Figure 9-8 Checking whether the CNAME record has taken effect



```
C:\Users\[redacted]>nslookup -qt=cname [redacted].com
Server:  anycast-dns.huawei.com
Address:  10.10.10.10

Non-authoritative answer:
videoinfo-push.hwcloudlive.com  canonical name = [redacted]c.cdnhwc3.com
```

9.5 Managing Domain Names

After an ingest domain name or streaming domain name is added, you can view basic information about the added domain names on the **Domains** page. You can disable, enable, or delete domain names, and disassociate them with each other.

Notes

If you add, modify, or delete a domain name, the change will be displayed in My Resources within 24 hours. Please check the data later.

Procedure

Step 1 Log in to the **Live console**.

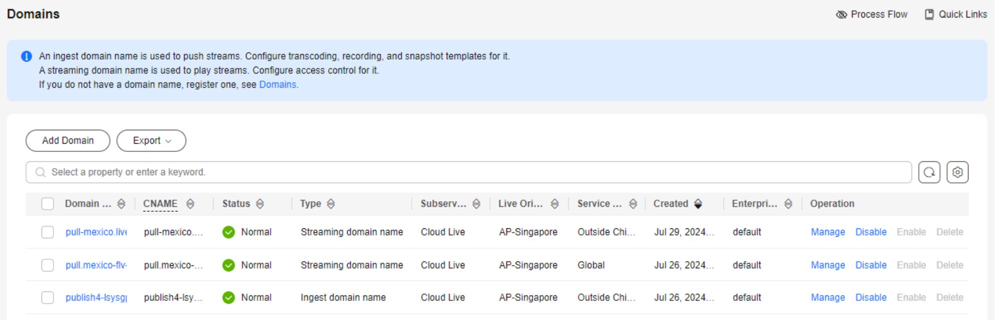
Step 2 In the navigation pane, choose **Domains**.

Step 3 Perform the following operations as required.

- View domain name details.

  In the domain list, you can view the CNAME record, type, status, and creation time of a domain name.

Figure 9-9 Domains



Domains

Process Flow Quick Links

An ingest domain name is used to push streams. Configure transcoding, recording, and snapshot templates for it.
A streaming domain name is used to play streams. Configure access control for it.
If you do not have a domain name, register one, see Domains.

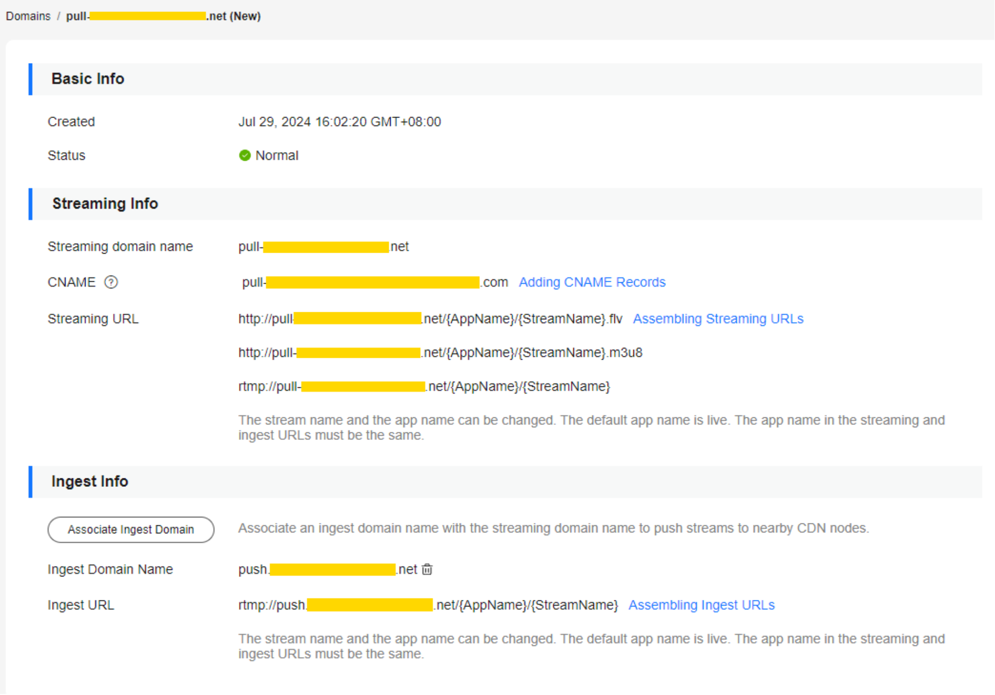
Add Domain Export

Select a property or enter a keyword.

	Domain ...	CNAME	Status	Type	Subserv...	Live Ori...	Service ...	Created	Enterpri...	Operation
□	pull-mexico.live	pull-mexico....	✓ Normal	Streaming domain name	Cloud Live	AP-Singapore	Outside Chi...	Jul 29, 2024...	default	Manage Disable Enable Delete
□	pull.mexico-flv-	pull.mexico-...	✓ Normal	Streaming domain name	Cloud Live	AP-Singapore	Global	Jul 26, 2024...	default	Manage Disable Enable Delete
□	publish4-lsysgj	publish4-lsy...	✓ Normal	Ingest domain name	Cloud Live	AP-Singapore	Outside Chi...	Jul 26, 2024...	default	Manage Disable Enable Delete

Click **Manage** in the **Operation** column of the desired domain name to view its basic information.

Figure 9-10 Domain information



Domains / pull-[redacted].net (New)

Basic Info

Created	Jul 29, 2024 16:02:20 GMT+08:00
Status	✓ Normal

Streaming Info

Streaming domain name	pull-[redacted]net
CNAME ⓘ	pull-[redacted].com Adding CNAME Records
Streaming URL	http://pull[redacted].net/{AppName}/{StreamName}.flv Assembling Streaming URLs http://pull-[redacted].net/{AppName}/{StreamName}.m3u8 rtmp://pull-[redacted].net/{AppName}/{StreamName} The stream name and the app name can be changed. The default app name is live. The app name in the streaming and ingest URLs must be the same.

Ingest Info

Associate Ingest Domain	Associate an ingest domain name with the streaming domain name to push streams to nearby CDN nodes.
Ingest Domain Name	push.[redacted].net
Ingest URL	rtmp://push.[redacted].net/{AppName}/{StreamName} Assembling Ingest URLs The stream name and the app name can be changed. The default app name is live. The app name in the streaming and ingest URLs must be the same.

- Disable a domain name.

  To disable a domain name, click **Disable** in the row that contains the target domain name. If the status changes to **Disabled**, the domain name has been disabled.

- Enable a domain name.

  To enable a disabled domain name, click **Enable** in the **Operation** column. If the status changes to **Normal**, the domain name has been enabled.

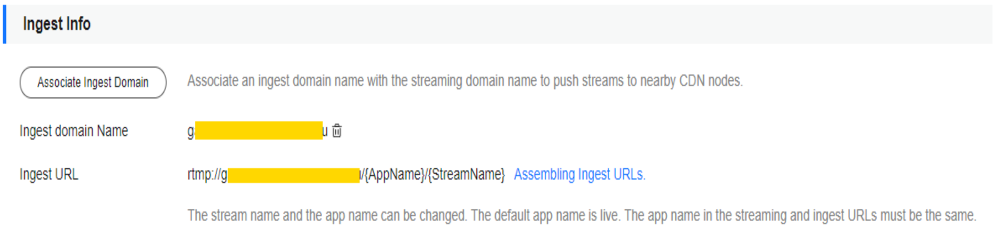
- Delete a domain name.

  Only a domain name in the **Disabled** status can be deleted. After disabling a domain name, click **Delete** in the row containing the domain name to delete it.

- Disassociate domain names.

If you want to disassociate an ingest domain name with a streaming domain name, click **Manage** in the **Operation** column of the streaming domain name. In the **Ingest Info** area, click 🗑.

Figure 9-11 Ingest Info



Ingest Info

Associate Ingest Domain

Associate an ingest domain name with the streaming domain name to push streams to nearby CDN nodes.

Ingest domain Name g[redacted]u 🗑

Ingest URL rtmp://g[redacted]/{AppName}/{StreamName} Assembling Ingest URLs.

The stream name and the app name can be changed. The default app name is live. The app name in the streaming and ingest URLs must be the same.

----End

9.6 Configuring a Geo-blocking Whitelist

By default, a user's IP address belongs to the acceleration area configured for the streaming domain name and can be used to pull streams from Live. To specify the areas that can be accessed by a streaming domain name, perform the operations described in this section.

Notes

- Huawei Cloud periodically updates IPv4 databases in all areas around the world. The geo-blocking whitelist configured here may not be able to identify all IP addresses. Terminals cannot identify a small number of IP addresses that are not in the databases. If high accuracy is required, exercise caution when using this function.
- If IP addresses in the databases cannot be accurately identified, the request may be scheduled to an unexpected billing area and billed in that area. For details, see **Product Pricing Details**.

Prerequisites

- A geo-blocking whitelist can only be configured for streaming domain names.
- Only one geo-blocking whitelist can be configured for each streaming domain name. The whitelist can be modified or deleted.

Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

Step 3 In the domain name list, find the streaming domain name whose geo-blocking needs to be specified and click **Manage** in the **Operation** column. The **Basic Info** page is displayed.

Step 4 In the navigation pane, choose **Templates** > **Geo-blocking**.

Step 5 Click **Add**. In the **Geo-blocking** dialog box that is displayed, select the areas where the streaming domain name can work and add them to **Selected Areas**.

Step 6 Click **OK**. The geo-blocking whitelist has been added.

After the whitelist is added, you can perform the following operations:

- Click **Edit** to change the areas that can be accessed by the streaming domain name.
- Click **Delete** to delete the whitelist.

----End

10 Stream Push

10.1 Assembling an Ingest URL

After domain names are configured, you can assemble an ingest URL and then push streams through the URL. You can also use the **tool** to quickly generate a signed URL of the ingest domain name.

Prerequisites

- You have **added an ingest domain name**.
- You have **configured CNAME records** at your domain names' DNS provider.
- To secure live resources, Live provides URL validation to encrypt and sign the ingest URL. If necessary, configure **URL validation** and push streams through the signed URL.

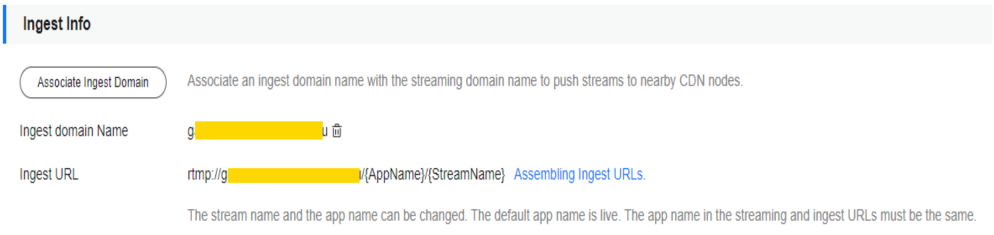
Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Manage** in the **Operation** column of the desired ingest domain name. On the displayed page, you can view the stream push information.

Figure 10-1 Ingest Info



Ingest Info

Associate Ingest Domain

Associate an ingest domain name with the streaming domain name to push streams to nearby CDN nodes.

Ingest domain Name g[redacted]u

Ingest URL rtmp://g[redacted]/{AppName}/{StreamName} Assembling Ingest URLs.

The stream name and the app name can be changed. The default app name is live. The app name in the streaming and ingest URLs must be the same.

- You need to customize **StreamName** to generate an ingest URL. For details, see **Original Ingest URL**.

- If URL validation is configured, you can add a signed string to the original ingest URL to generate a new ingest URL. For details, see **Signed Ingest URL**.

----End

Original Ingest URL

Assembling rules

Ingest URL format:

```
rtmp://Ingest domain name/AppName/StreamName
```

- *Ingest domain name* is the one you added on the Live console.
- *AppName*: application name. The default value is **live**. You can customize the application name. Only letters, digits, underscores (_), and hyphens (-) are allowed.
- *StreamName*: live stream name. Multiple live streams can be created for each application. You can customize the stream name, for example, huawei1.

Examples

If the added ingest domain name is **test-push.example.com**, *AppName* is **livetest**, and *StreamName* is **huawei1**, the ingest URL is:

```
rtmp://test-push.example.com/livetest/huawei1
```

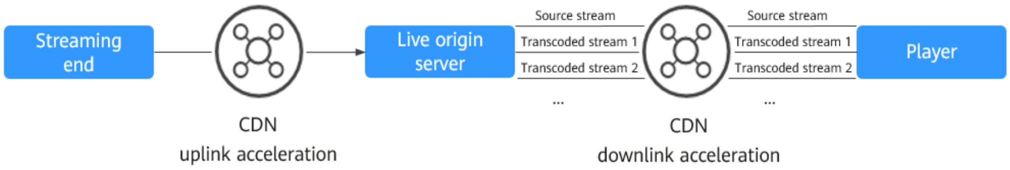
Signed Ingest URL

If **URL validation** is configured, you must assemble a signed URL based on obtained authentication information and then push streams through the signed URL. For details, see **URL Validation**.

10.2 Transcoding

You can transcode livestreams into video streams with different resolutions and bitrates to meet a broad range of requirements.

Figure 10-2 Transcoding architecture



Function Overview

The transcoding function allows you to:

- Transcode source audio and video into one or more formats for playback on a wide range of devices.
- Adapt the output bitrate to different network bandwidths.
- Reduce the costs of distributing livestreams. H.265 codec and low-bitrate HD can reduce the bitrate by about 20% at the same resolution.

- Customize a transcoding template, including ID, resolution, bitrate, and frame rate.

Notes

- You can configure multiple transcoding templates for one domain name. After a transcoding request is received, a transcoding template in which **AppName** is the same as that in the request URL takes effect. If you do not need transcoding, **delete the transcoding template** before stream push.
- The transcoding rule of the live stream takes effect when the live stream is started. If the transcoding configuration is modified, the modification does not take effect for the ongoing live stream. The modification takes effect only for the live stream that is pushed after the modification.
- Low-bitrate HD is disabled by default. If you enable it, you will be charged based on the **rates of low-bitrate HD**.
- Upsampling is not supported. If the resolution set in a transcoding template is higher than source resolution, the video can be played, but the resolution of the played video is source resolution.

Prerequisites

- You have **added an ingest domain name**.
- You have **configured CNAME records** at your domain names' DNS provider.

Pricing Notes

The transcoding function is a billing item. You are charged based on a combination of the codec, output resolution, and length of an output video. Standard transcoding and low-bitrate HD transcoding are billed differently. For details about the transcoded output resolution, see the **Output Resolution** column in the **Live Transcoding** area in **Live Pricing Details**.

Creating a Transcoding Template

You can customize a template on the Live console or by calling a **Live API**. If you want to play transcoded live TV streams, obtain a transcoded streaming URL. For details, see **Transcoded Streaming URL**.

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

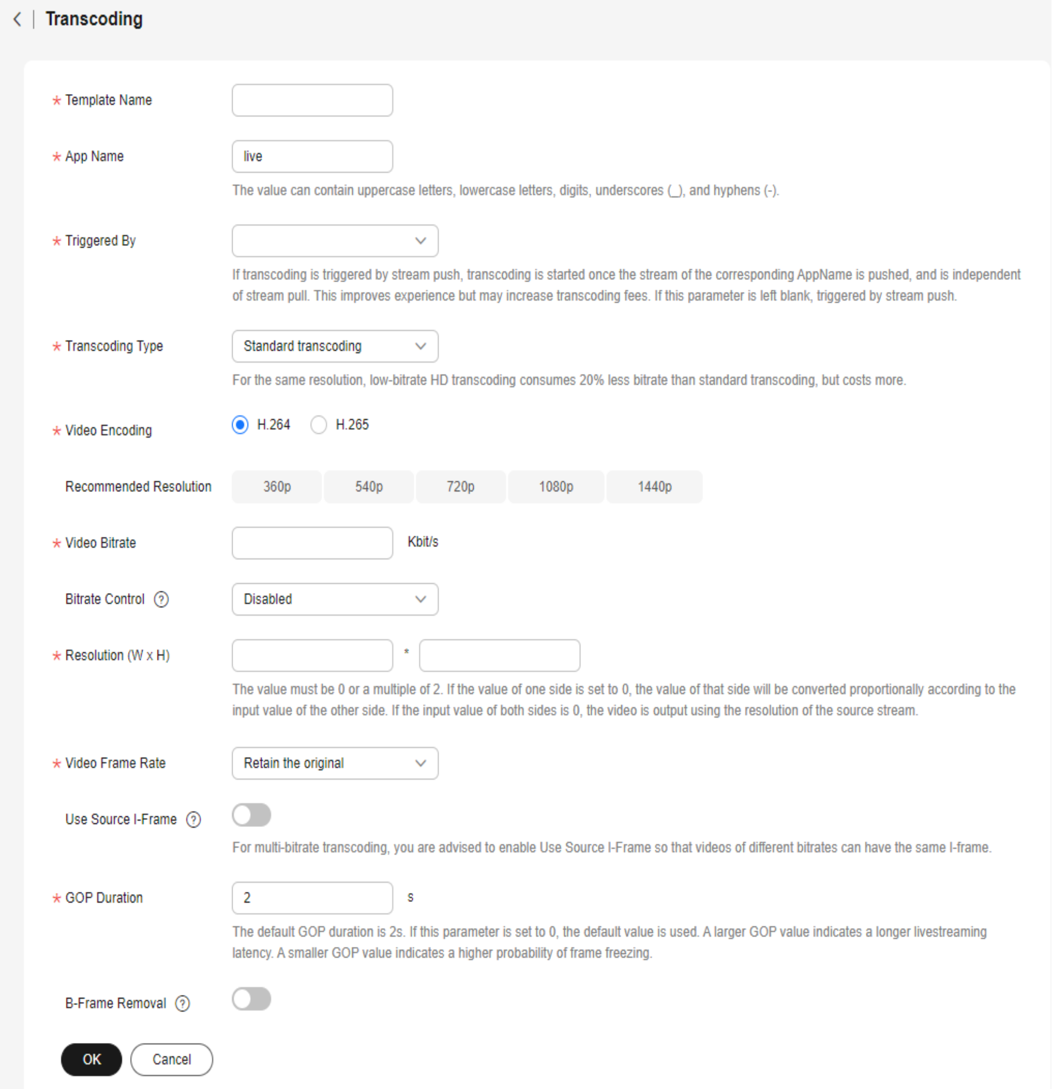
Step 3 Click **Manage** in the **Operation** column of the desired ingest domain name.

Step 4 In the navigation pane, choose **Templates** > **Transcoding** to view the transcoding template information.

Step 5 Click **Create Transcoding Template**. A page like **Figure 10-3** is displayed.

Configure transcoding parameters as instructed by **Table 10-1**.

Figure 10-3 Creating a transcoding template



Transcoding

* Template Name

* App Name: live

The value can contain uppercase letters, lowercase letters, digits, underscores (_), and hyphens (-).

* Triggered By

If transcoding is triggered by stream push, transcoding is started once the stream of the corresponding AppName is pushed, and is independent of stream pull. This improves experience but may increase transcoding fees. If this parameter is left blank, triggered by stream push.

* Transcoding Type: Standard transcoding

For the same resolution, low-bitrate HD transcoding consumes 20% less bitrate than standard transcoding, but costs more.

* Video Encoding: ● H.264 ○ H.265

Recommended Resolution: 360p 540p 720p 1080p 1440p

* Video Bitrate: Kbit/s

Bitrate Control: Disabled

* Resolution (W x H): *

The value must be 0 or a multiple of 2. If the value of one side is set to 0, the value of that side will be converted proportionally according to the input value of the other side. If the input value of both sides is 0, the video is output using the resolution of the source stream.

* Video Frame Rate: Retain the original

Use Source I-Frame

For multi-bitrate transcoding, you are advised to enable Use Source I-Frame so that videos of different bitrates can have the same I-frame.

* GOP Duration: 2 s

The default GOP duration is 2s. If this parameter is set to 0, the default value is used. A larger GOP value indicates a longer livestreaming latency. A smaller GOP value indicates a higher probability of frame freezing.

B-Frame Removal

Table 10-1 Transcoding template parameters

Parameter	Description
Template Name	Name of a transcoding template.
App Name	Application name. The default value is **live**. You can customize the application name. Only letters, digits, underscores (_), and hyphens (-) are allowed.

Parameter	Description
Triggered By	Indicates how live transcoding is triggered. When a transcoding request is received, the transcoding template whose name is the same as the value of **AppName** in the request address takes effect and transcoding starts. ● **Stream pull**: The transcoding task of the corresponding template is triggered only when a transcoded stream is played. ● **Stream push**: The transcoding task of the corresponding template is triggered only when a stream is pushed. This mode means longer transcoding duration and increasing fees. Default value: **Stream pull** **CAUTION** The transcoding templates under an *AppName* support only one triggering mode. If there are multiple transcoding templates, exercise caution when changing the value of **Triggered By** for the transcoding templates. For example, if the value of **Triggered By** of a template is changed from **Stream push** to **Stream pull**, the value of **Triggered By** of all transcoding templates under the *AppName* will be changed to **Stream pull**.
Transcoding Type	Live transcoding type. Options: ● **Standard transcoding** ● **Low-bitrate HD** For the same resolution, low-bitrate HD transcoding consumes 20% less bitrate than standard transcoding but costs more. Low-bitrate HD means that the output bitrate is lower at a given image quality. If you enable this option, you will be billed based on the **rates of low-bitrate HD**.
Video Encoding	H.264 and H.265 are supported.
Recommended Resolution	Screen resolution. After the resolution level is selected, the **Video Bitrate** and **Resolution (W x H)** parameters are automatically set and the recommended values are provided. You can also change the values as needed.
Video Bitrate	Average bitrate of the transcoded video, in kbit/s. Value range: 40 to 30,000

Parameter	Description
Bitrate Control	Bitrate control policy. Options: ● **Disabled**: Bitrate adaptation is disabled. The target bitrate is output as specified. ● **Not higher than source stream**: The target bitrate is the smaller value between the specified bitrate and the bitrate of the source file. That is, the bitrate does not increase. ● **Adaptive to source stream**: The target bitrate is adaptive to the bitrate of the source file.
Resolution (W x H)	Width and height of the video, in pixel. If both the width and height are set to **0**, the output resolution is the same as that of the source. If only the width or height is set to **0**, the output resolution will be scaled based on the value of the side that is not set to **0**. Value range: ● **Width**: The value must be 0 or a multiple of 2 from 32 to 3,840. ● **Height**: The value must be 0 or a multiple of 2 from 32 to 2,160.
Video Frame Rate	Frame rate of the transcoded video. Options: ● **Retain the original** ● **Set a new one**: If you select this option, you need to enter the frame rate. The value ranges from 0 to 60. If the value is set to **0**, the frame rate is adaptive.
Use Source I-Frame	Policy for outputting I-frames during encoding. ● If this function is disabled, I-frames are output based on the configured GOP duration. ● If this function is enabled, the output I-frames are the same as those of the source. That is, if the source contains I-frames, I-frames are output after encoding. If the source does not contain I-frames, non-I-frames are output after encoding. If this function is enabled, the GOP duration setting is invalid. For multi-bitrate transcoding, you are advised to enable **Use Source I-Frame** so that videos of different bitrates can have the same I-frame.

Parameter	Description
GOP Duration	I-frame interval by time, in second. The value ranges from 0 to 10 and defaults to **2**. If the value is not **0**, the I-frame interval is set based on the GOP duration. If the value is **0**, the default value is used. A larger GOP duration value indicates a longer livestreaming latency. A smaller GOP duration value indicates a higher probability of frame freezing.
B-Frame Removal	After this function is enabled, the transcoded video does not contain B-frames.

Step 6 Click **OK**.

A transcoding template is added on the live transcoding page.

Step 7 Obtain a transcoded streaming URL if you need to stream your video via a transcoded streaming URL. For details, see **Transcoded Streaming URL**.

----End

Transcoding Template Management

You can perform the following operations on your transcoding template:

- Edit a transcoding template.

  Click **Edit** in the **Operation** column to modify parameters in the template. The value of **AppName** cannot be changed.

  ⚠ CAUTION

  The transcoding rule of the live stream takes effect when the live stream is started. If the transcoding configuration is modified, the modification does not take effect for the ongoing live stream. The modification takes effect only for the live stream that is pushed after the modification.

- Delete a transcoding template.

  Click **Delete** in the **Operation** column.

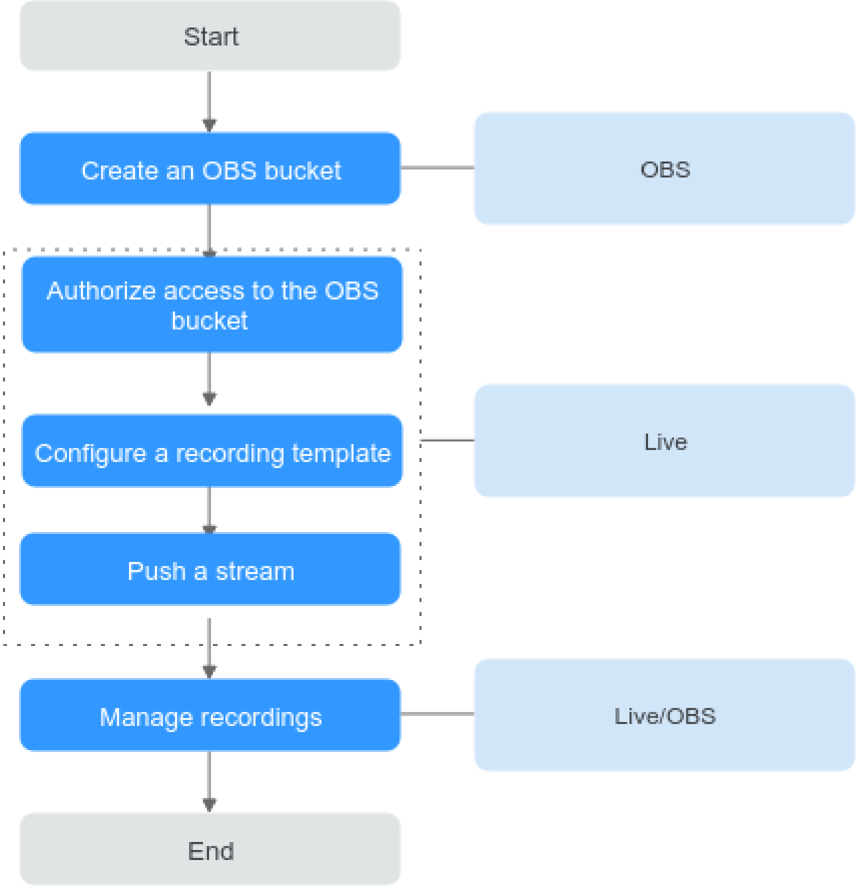
10.3 Recording Live Video to OBS

10.3.1 Creating a Recording Template

Live allows you to record a livestream and store the recording in OBS, where you can download and share the recording.

Figure 10-4 shows the process of recording and storing a live video in OBS.

Figure 10-4 Process of recording and storing a live video in OBS



1. **(Optional) Create an OBS bucket** for storing recordings. If you already have one, go to **2**.

   NOTE

   The created OBS bucket must be in the same region as Live.

2. **Authorize access to the OBS bucket** so that the system can save the recordings in the OBS bucket.

   NOTE

   - Authorizing access to an OBS bucket is allowed only under a Huawei Cloud account, but not allowed for **IAM users**.
   - The OBS bucket that Live is authorized to access must be in the same region as Live.
   - If you want to cancel the authorization of access to a bucket, check whether there are recordings or screenshots in the bucket. If there are, the recordings or screenshots will be removed from the bucket after the authorization is canceled.

3. **Configure a recording template**. The recording template in which **AppName** and **StreamName** are the same as those in the ingest URL takes effect, and recordings are stored in OBS based on template settings. You can set a callback address to get notifications about the recording status.
4. Push a stream through an ingest URL and record the livestream based on a configured recording template. For details about how to create an ingest URL, see **Assembling an Ingest URL**.

5. **Manage recordings**. You can view basic information about recordings on the Live console, and manage recordings, such as preview, sharing, and deletion, on the OBS console.

   NOTE

   The resolution of recordings is the same as that of the pushed streams.

Notes

- Recording rules can be configured at domain name, application, and stream levels. Rules at the stream level take effect first. Rules at the same level must have the same recording type.
- Recordings cannot be deleted from Live because Live does not store recordings. Live logs recording events and store them for 30 days. You can manually delete recordings from OBS or configure **OBS lifecycle management rules** to set a retention period and policy for recordings.
- If stream push is interrupted due to network jitter during live recording, recording stops. When stream push resumes, recording restarts accordingly.
- Recording starts when stream push starts and stops until stream push ends. Recording cannot be stopped or started during stream push. If the recording template is deleted during stream push, recording continues until stream push ends.
- Ensure that OBS is not suspended due to arrears. Otherwise, recording will fail. You are advised to **buy an OBS package**.
- Only input livestreams can be recorded. Transcoded livestreams cannot be recorded.

Prerequisites

- You have **added an ingest domain name**.
- You have **configured CNAME records** at your domain names' DNS provider.
- Recordings are stored in OBS. You must **enable OBS** before storing recordings in OBS.

Pricing Notes

- **Live recording fees** are charged by Live.
- Live recordings are stored in OBS. Therefore, OBS charges you for the storage. See **OBS Pricing Details**.

Step 1: (Optional) Create an OBS Bucket

If you have not created an OBS bucket, **create one**. If you already have one, go to **Step 2: Authorize Access to the OBS Bucket**.

Step 2: Authorize Access to the OBS Bucket

Authorize Live to store recordings in OBS buckets.

CAUTION

After access to the OBS bucket is authorized, Live can access the OBS bucket. Ensure that the bucket processes only workloads related to Live. Do not store confidential files in the bucket.

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **OBS Authorization**.

Step 3 Under the **Live** tab, click **Authorize** in the **Operation** column of the desired OBS bucket.

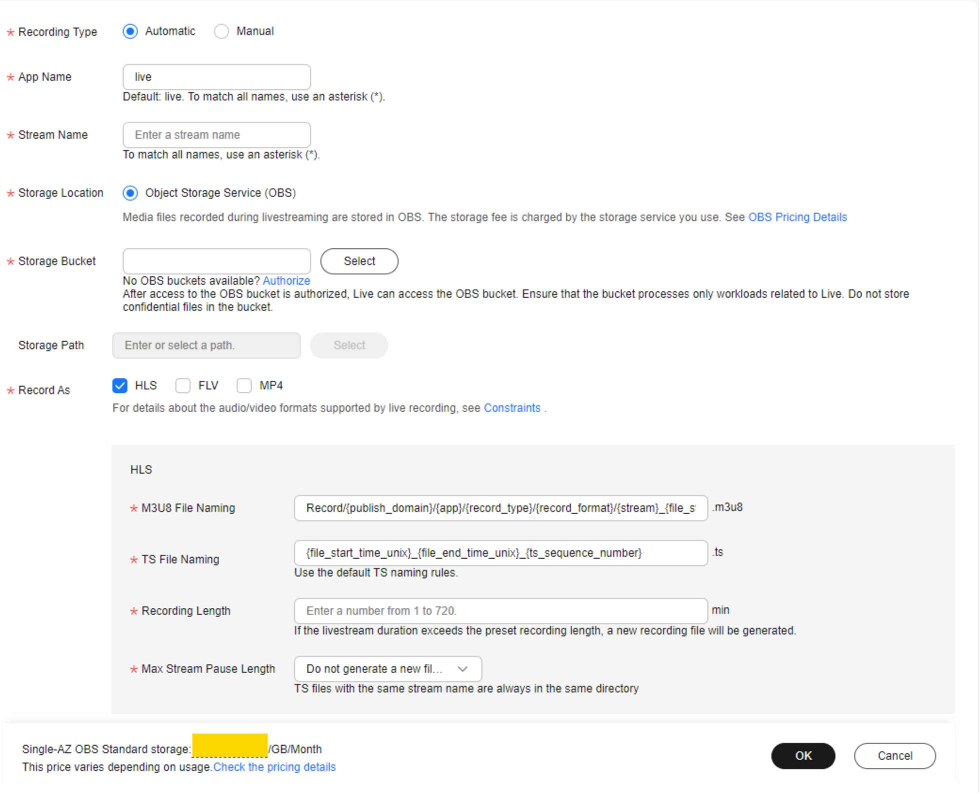
----End

Step 3: Configure a Recording Template

If you want to record a livestream for replay, configure a recording template. The recording template in which **App Name** and **Stream Name** are the same as those in the ingest URL takes effect.

1. Log in to the **Live console**.
2. In the navigation pane, choose **Domains**.
3. Click **Manage** in the **Operation** column of the desired ingest domain name.
4. In the navigation pane, choose **Templates** > **Recording (New)**.
5. Click **Create Recording Template**.
6. Configure recording parameters. **Table 10-2** describes the parameters.

Figure 10-5 Configuring recording parameters



* Recording Type ● Automatic ○ Manual

* App Name: live
Default: live. To match all names, use an asterisk (*).

* Stream Name: Enter a stream name
To match all names, use an asterisk (*).

* Storage Location ● Object Storage Service (OBS)
Media files recorded during livestreaming are stored in OBS. The storage fee is charged by the storage service you use. See OBS Pricing Details

* Storage Bucket: Select
No OBS buckets available? Authorize
After access to the OBS bucket is authorized, Live can access the OBS bucket. Ensure that the bucket processes only workloads related to Live. Do not store confidential files in the bucket.

Storage Path: Enter or select a path. Select

* Record As ☑ HLS □ FLV □ MP4
For details about the audio/video formats supported by live recording, see Constraints .

HLS

* M3U8 File Naming: Record/{publish_domain}/{app}/{record_type}/{record_format}/{stream}_{file_s .m3u8

* TS File Naming: {file_start_time_unix}_{file_end_time_unix}_{ts_sequence_number} .ts
Use the default TS naming rules.

* Recording Length: Enter a number from 1 to 720. min
If the livestream duration exceeds the preset recording length, a new recording file will be generated.

* Max Stream Pause Length: Do not generate a new fil...
TS files with the same stream name are always in the same directory

Single-AZ OBS Standard storage: [redacted] /GB/Month
This price varies depending on usage.Check the pricing details

Table 10-2 Recording parameters

Parameter	Description
Recording Type	● **Automatic**: The recording automatically starts when livestreams that meet the configured recording template are pushed. ● **Manual**: When livestreams that meet the configured recording template are pushed, you can call the API for to start or stop recording livestreams. **NOTE** ● The recording type cannot be changed once configured. ● Only when livestreams are pushed, can the API for submitting a recording command be called. ● Manual recording supports only recording start and stop for a specific stream. Even if the recording rule is at the domain name level, the stream name must be specified when you deliver the recording start and stop commands. ● To manually stop recording, you can set **Maximum Stream Pause Length** when configuring the recording rule, so that recording will stop when the stream has been paused beyond the time indicated by **Maximum Stream Pause Length**. You can also call an API to stop recording. ● After the command for stopping recording is manually delivered, it takes a period of time to clear resources for the recording task. If the command for starting recording is delivered again shortly after the stop command is delivered, a message indicating that the recording task is not complete may be returned.
App Name	Application name. The default value is **live**. You can customize the application name. Only letters, digits, underscores (_), and hyphens (-) are allowed. If this parameter is set to *****, the recording template applies to all applications under the domain name.
Stream Name	Livestream name. If this parameter is set to *****, the recording template applies to all livestreams with the same *App Name*.
Storage Location	Where recordings are stored
Storage Bucket	OBS bucket where recordings are stored
Storage Path	OBS path where recordings are stored To change the path later, click **Edit** in the **Operation** column of the row containing the template in the recording template list.
Record As	Format of a recording. Live videos can be recorded in HLS, FLV, or MP4 format.

Parameter	Description
HLS	**M3U8 File Naming**: The storage path and file name prefix need to be specified. `Record/{publish_domain}/{app}/{record_type}/{record_format}/{stream}_{file_start_time}/{stream}_{file_start_time}` Parameter description: ● **Record**: Retain the default value. ● **publish_domain**: the ingest domain name added on the Live console ● **app**: application name, which defaults to **live** ● **record_type**: value of **Recording Type** on the current page ● **record_format**: value of **Record As** on the current page ● **stream**: livestream name
	TS File Naming: The file name prefix needs to be specified. `{file_start_time_unix}_{file_end_time_unix}_{ts_sequence_number}`
	Recording Length: Its value ranges from 1 to 720 minutes. If a live video has been recorded for more than 12 hours, a new M3U8 file will be created based on the naming rule.
	Options of **Max Stream Pause Length**: ● **Generate a new file when a stream is paused** ● **Do not generate a new file when a stream is paused** ● **Other**: If the interruption duration of a livestream exceeds the specified range, a new recording file is generated. The maximum value of **Max Stream Pause Length** is 300s.
FLV	**File Naming**: The storage path and file name prefix need to be specified. `Record/{publish_domain}/{app}/{record_type}/{record_format}/{stream}_{file_start_time}/{file_start_time}` Parameter description: ● **Record**: Retain the default value. ● **publish_domain**: the ingest domain name added on the Live console ● **app**: application name, which defaults to **live** ● **record_type**: value of **Recording Type** on the current page ● **record_format**: value of **Record As** on the current page ● **stream**: livestream name
	Recording Length: Its value ranges from 1–360 minutes. If a live video has been recorded for more than six hours, a new file will be created based on the naming rule.

Parameter	Description
	Options of **Max Stream Pause Length**: ● **Generate a new file when a stream is paused** ● **Other**: If the interruption duration of a livestream exceeds the specified range, a new recording file is generated.
MP4	**File Naming**: The storage path and file name prefix need to be specified. `Record/{publish_domain}/{app}/{record_type}/{record_format}/{stream}_{file_start_time}/{file_start_time}` Parameter description: ● **Record**: Retain the default value. ● **publish_domain**: the ingest domain name added on the Live console ● **app**: application name, which defaults to **live** ● **record_type**: value of **Recording Type** on the current page ● **record_format**: value of **Record As** on the current page ● **stream**: livestream name
	Recording Length: Its value ranges from 1–360 minutes. If a live video has been recorded for more than six hours, a new file will be created based on the naming rule.
	Options of **Max Stream Pause Length**: ● **Generate a new file when a stream is paused** ● **Other**: If the interruption duration of a livestream exceeds the specified range, a new recording file is generated.

NOTE

If livestream push is normal, the time when HLS recordings are generated in the OBS bucket is related to the keyframe interval configured on the player. By default, the first recording is generated after three keyframe intervals (6 seconds). An FLV or MP4 recording is generated only after the recording ends.

The value of **Max Stream Pause Length** affects the triggering of the recording callback event **RECORD_FILE_COMPLETE**.

- **Do not generate a new file when a stream is paused**: When the recording duration reaches the configured recording length, a recording file is generated and the recording callback event is triggered.
- **Generate a new file when a stream is paused**: Every time a stream is interrupted, a new recording file is generated and the recording callback event is triggered.
- **Other**: Every time the stream interruption duration reaches the specified value, a new recording file is generated and the recording callback event is triggered. If the stream interruption duration does not reach the specified value and the recording duration reaches the configured recording length, a recording file is generated and the recording callback event is triggered.

7. Click **OK**.

   You can create multiple recording templates. The recording template in which **App Name** and **Stream Name** are the same as those in the ingest URL takes effect.

8. Obtain an **ingest URL** to **push streams**.

   The resolution and bitrate of the generated recordings are the same as those of the livestream.

You can **manage recordings** on the OBS console, such as preview, download, and share.

Modifying or Deleting a Recording Template

You can perform the following operations on your recording template:

- Editing a recording template

  Click **Edit** in the **Operation** column of the row containing the target recording template in the template list to edit the template.

  The recording type cannot be changed.

- Deleting a recording template

  Click **Delete** in the **Operation** column of the row containing the target recording template in the template list to delete the template.

10.3.2 Configuring a Recording Callback

You can configure an HTTP/HTTPS URL to receive recording status feedback. The system will send POST requests in JSON format to your server, so that you can know the recording status.

Prerequisites

- You have **added an ingest domain name**.
- You have **configured CNAME records** at your domain names' DNS provider.

Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

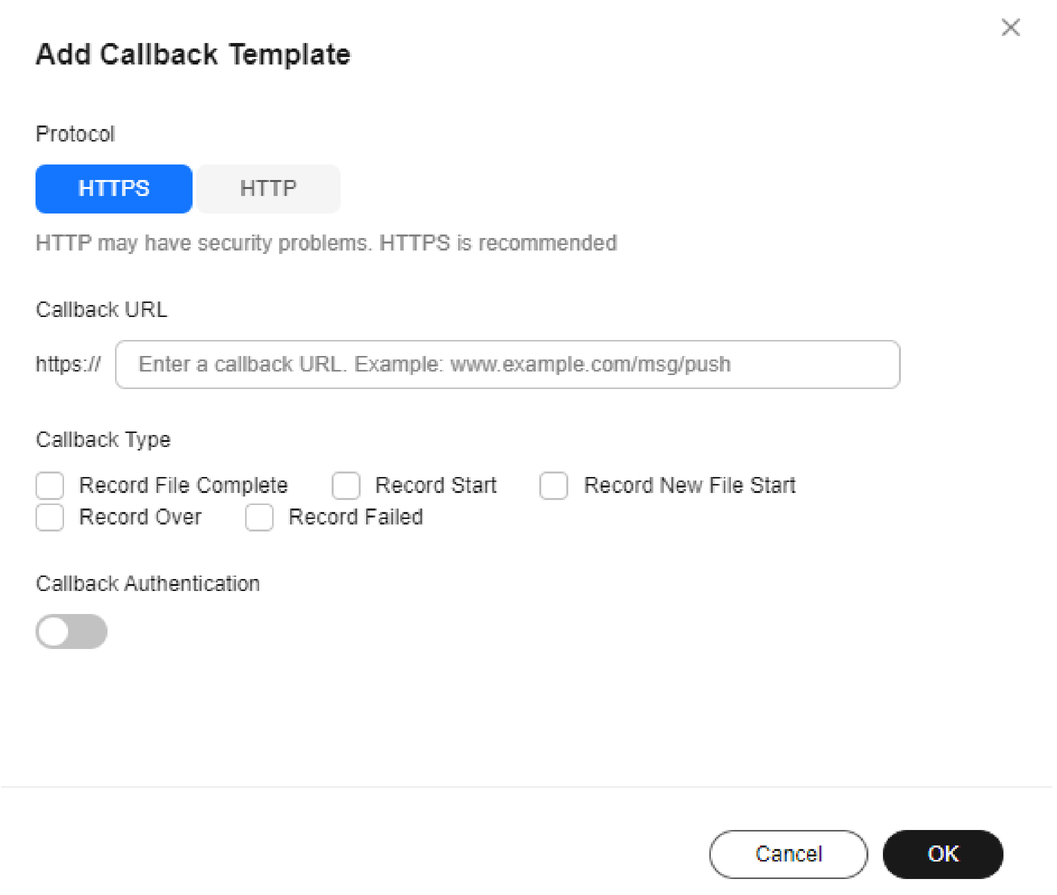
Step 3 Click **Manage** in the **Operation** column of the desired ingest domain name.

Step 4 In the navigation pane, choose **Templates** > **Recording (New)**.

Step 5 Click **Create Callback Template**.

In the displayed dialog box, enter a callback URL, as shown in **Figure 10-6**. **Table 10-3** describes the callback parameters.

Figure 10-6 Adding a callback URL



Add Callback Template

Protocol

HTTPS | HTTP

HTTP may have security problems. HTTPS is recommended

Callback URL

https:// Enter a callback URL. Example: www.example.com/msg/push

Callback Type

□ Record File Complete □ Record Start □ Record New File Start
□ Record Over □ Record Failed

Callback Authentication

Table 10-3 Recording callback parameters

Parameter	Description
Protocol	A callback URL supports HTTP and HTTPS. HTTPS is more secure than HTTP and is recommended.

Parameter	Description
Callback URL	The callback URL cannot contain message headers or parameters. Only the HTTP/HTTPS protocol is supported. HTTPS is recommended.
Callback Type	When callback messages are sent. The options are as follows: ● Record File Complete ● Record Start ● Record New File Start ● Record Over ● Record Failed For details about callback types, see **Table 10-4**.
Callback Authentication	If this function is enabled, you need to configure **Authentication Algorithm** and **Authentication Key**.
Authentication Algorithm	The encrypted content in callback messages varies depending on the authentication algorithm. MD5 is not secure and HMACSHA256 is recommended. ● **MD5**: MD5(*key* + *auth_timestamp*) ● **HMACSHA256**: HMACSHA256(*auth_timestamp* + *event_type* + *publish_domain* + *app* + *stream* + *download_url* + *play_url*, *key*)
Authentication Key	The value can be customized and consist of at least 32 characters in digits and letters.

----End

Editing or Deleting a Recording Callback

You can perform the following operations on your recording callback:

- Editing a recording callback

  Click **Edit** in the **Operation** column of the row containing the target recording callback in the callback list to edit the callback.

- Deleting a recording callback

  Click **Delete** in the **Operation** column of the row containing the target recording callback in the callback list to delete the callback.

Callback Example

Table 10-4 describes the fields in a callback message body.

```
{
   "project_id": "70b76xxxxxx34253880af501cdxxxxxx",
   "job_id": "dc0a1773-0cef-xxxx-xxxx-9a38fdb095d2",
   "task_id": "51126d0ebe94b1da00d2e21a10xxxxxx",
   "event_type": "RECORD_FILE_COMPLETE",
   "publish_domain": "push.example.com",
   "app": "live",
   "stream": "mystream",
   "record_format": "HLS",
   "download_url": "https://obs.cn-north-4.myhuaweicloud.com/live/record-xxxx-mystream-1589967495/
record-push.example.com-live-mystream-1589967495.m3u8",
   "asset_id": "1a0d8e9bfaexxxxxxbe5021e62aa1e96",
   "file_size": 3957964,
   "record_duration": 120,
   "start_time": "2020-03-08T14:10:25Z",
   "end_time": "2020-03-08T14:12:25Z",
   "width": 1280,
   "height": 720,
   "obs_location": "https://obs.cn-north-4.myhuaweicloud.com",
   "obs_bucket": "mybucket",
   "obs_object": "live/record-xxxx-mystream-1589967495/record-hwpublish.myun.tv-live-
mystream-1589967495.m3u8",
   "auth_sign": "4f97f46759axxxxxx7ad21e9935dc175",
   "auth_timestamp": 1583676745
}
```

Table 10-4 Message body

Field	Description
project_id	Project ID.
job_id	Name of a file. This parameter is carried when the value of **event_type** is **RECORD_NEW_FILE_START** or **RECORD_FILE_COMPLETE**.
task_id	Recording task ID, which uniquely identifies a recording task.

Field	Description
event_type	Message type. Options: ● **RECORD_START**. This event is triggered when you start recording. ● **RECORD_NEW_FILE_START**. This event is triggered in either of the following scenarios: – The system starts creating the first recording file. – After a live stream is resumed, if **Maximum Stream Pause Length** is set to **Generate a new file after a stream is paused.**, the system starts to create a recording file. – If the current recording duration exceeds the configured one, the system starts to create another recording file. ● **RECORD_FILE_COMPLETE**. This event is triggered in either of the following scenarios: – When the recording duration reaches the configured recording length, a recording file has been generated. The system starts creating a new recording file. – After a live stream is interrupted, if **Maximum Stream Pause Length** is set to **Generate a new file after a stream is paused.**, a recording file has been created. Once the stream is resumed, the system will start creating a new recording file. ● **RECORD_OVER**. This event is triggered when a live stream has been paused beyond the time indicated by **Maximum Stream Pause Length** and a recording has been created. ● **RECORD_FAILED**. This event is triggered when stream pulling fails or uploading recordings to OBS fails.
publish_domain	Ingest domain name.
app	Application name.
stream	Stream name.
record_format	Recording format. The HLS, FLV, and MP4 formats are supported.

Field	Description
download_url	Address to download the recording. This parameter is used only when **event_type** is **RECORD_FILE_COMPLETE**. **NOTE** The quality of video playback using the download address cannot be guaranteed.
asset_id	Name of a recording file This parameter is used only when **event_type** is **RECORD_FILE_COMPLETE**.
file_size	File size. Unit: byte
record_duration	Duration of a recording. Unit: second
start_time	Start time of a recording, which is, time when the first frame is received. The format is yyyy-mm-ddThh:mm:ssZ. This parameter is used only when **event_type** is **RECORD_FILE_COMPLETE**.
end_time	End time of a recording. The format is yyyy-mm-ddThh:mm:ssZ. This parameter is used only when **event_type** is **RECORD_FILE_COMPLETE**.
width	Width of a video recording This parameter is used only when **event_type** is **RECORD_FILE_COMPLETE**.
height	Height of a recording. This parameter is used only when **event_type** is **RECORD_FILE_COMPLETE**.
obs_location	Region where the OBS bucket for storing the recording is located. This parameter is used only when **event_type** is **RECORD_FILE_COMPLETE**.
obs_bucket	OBS bucket where recordings are stored. This parameter is used only when **event_type** is **RECORD_FILE_COMPLETE**.
obs_object	OBS path where recordings are stored. This parameter is used only when **event_type** is **RECORD_FILE_COMPLETE**.

Field	Description
auth_sign	Event notification signature. This parameter is carried when an authentication key is configured. ● MD5: **auth_sign** = MD5(*key* + *auth_timestamp*) ● **HMACSHA256**: HMACSHA256(*auth_timestamp* + *event_type* + *publish_domain* + *app* + *stream* + *download_url* + *play_url*, *key*) *key* indicates the key used for authentication.
auth_timestamp	UNIX timestamp when the event notification signature expires. This parameter is carried when an authentication key is configured. The value is a decimal Unix timestamp, that is, the number of seconds that have elapsed since January 1, 1970 00:00:00 UTC/GMT. If the time specified by **auth_timestamp** has expired, the notification will become invalid to avoid network replay attacks.
error_message	Description about a failed recording. This parameter is used only when **event_type** is **RECORD_FAILED**.

10.3.3 Managing Recordings

When the live recording is complete, view recordings on the OBS console.

Managing Recordings Using the OBS Console

Step 1 In the navigation pane of the OBS console, choose **Object Storage**.

Step 2 In the bucket list, click the bucket that stores recordings.

On the page displayed, you can download and share the recordings.

----End

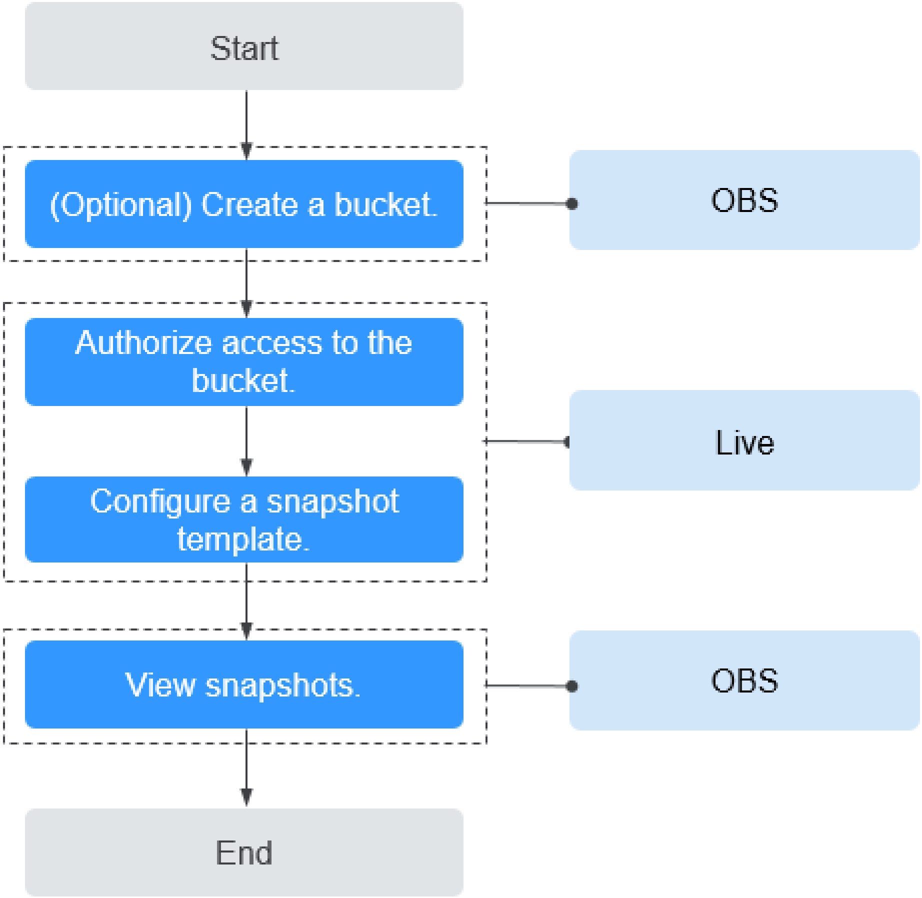
10.4 Snapshot Capturing

Live captures snapshots from a livestream based on a configured template and stores the captured snapshots in an OBS bucket. Multiple snapshot templates can be configured for an ingest domain name. The template in which *App Name* is the same as that in the ingest URL takes effect.

Process Flow

Figure 10-7 shows the process for configuring a snapshot template.

Figure 10-7 Process for configuring a snapshot template


Start
(Optional) Create a bucket.
OBS
Authorize access to the bucket.
Live
Configure a snapshot template.
View snapshots.
OBS
End

1. **(Optional) Create an OBS bucket** for storing live video snapshots. If you already have one, go to **2**.

   NOTE

   The OBS bucket for storing live video snapshots must be in the same region as the Live service. For example, if you use Live in the **CN North-Beijing4** region, then snapshots must be stored in an OBS bucket in the **CN North-Beijing4** region.

2. **Authorize access to the OBS bucket** so that the system can save the snapshots in the OBS bucket.
3. **Configure a snapshot template** to capture snapshots from a video stream at a specified interval and save them as JPG files in an authorized OBS bucket.
4. **View snapshots** in the output path.

Notes

- Live and the OBS bucket for storing snapshots must be in the same region.
- You are advised to set the OBS bucket as a private bucket. The differences between a private bucket and a public bucket are as follows:

  - Private bucket: You must add authentication information before accessing the bucket and downloading snapshots. For details about the authentication information, see **Creating a Signed URL (SDK for Go)**.
  - Public bucket: You can directly access the bucket and download snapshots.
- Multiple snapshot templates can be configured for a domain name. The snapshot template in which *App Name* is same as that in the ingest URL takes effect.
- Only JPG files can be generated.
- Huawei Cloud Live plans to bring offline the function of carrying authentication information in a snapshot callback URL on August 15, 2024.

Prerequisites

- You have **added an ingest domain name**.
- You have **configured CNAME records** at your domain names' DNS provider.
- Snapshots are stored in OBS. You must **enable OBS** before storing recordings in OBS.

Pricing Notes

- **Snapshot capturing** is a billing item. You are billed based on the number of snapshots.
- Snapshots are stored in OBS. **OBS** charges you for the storage.

Step 1: (Optional) Create an OBS Bucket

If you have not created an OBS bucket, **create one** in the region of Live. If you already have one, go to **Step 2: Authorize Access to the OBS Bucket**.

Step 2: Authorize Access to the OBS Bucket

Perform the following steps to authorize Live to store snapshots in your OBS bucket.

⚠ CAUTION

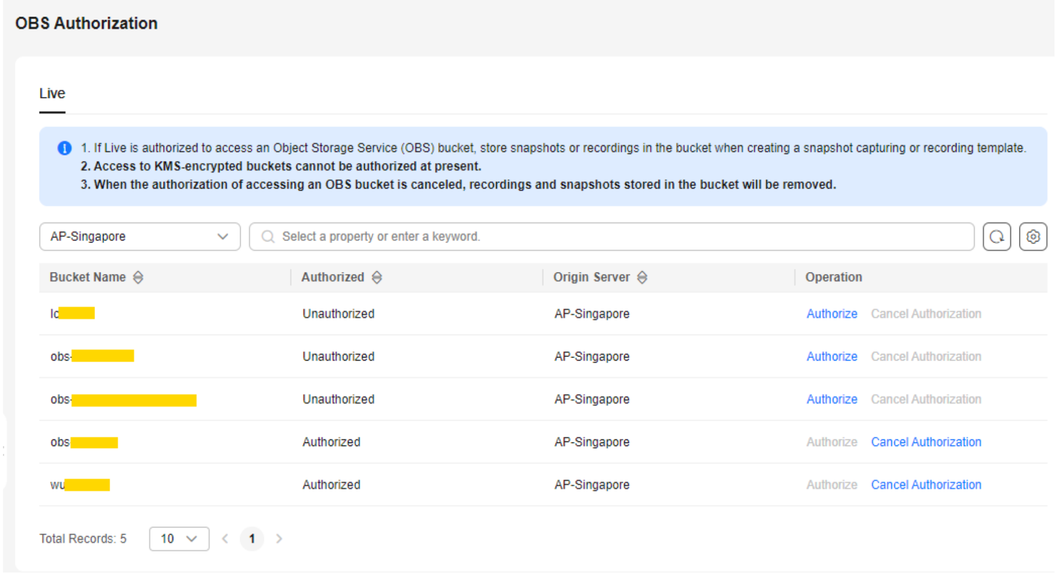
After access to the OBS bucket is authorized, Live can access the OBS bucket. Ensure that the bucket processes only workloads related to Live. Do not store confidential files in the bucket.

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **OBS Authorization**.

Step 3 Under the **Live** tab, click **Authorize** in the **Operation** column of the desired OBS bucket.

Figure 10-8 OBS authorization



OBS Authorization

Live

1. If Live is authorized to access an Object Storage Service (OBS) bucket, store snapshots or recordings in the bucket when creating a snapshot capturing or recording template.
2. Access to KMS-encrypted buckets cannot be authorized at present.
3. When the authorization of accessing an OBS bucket is canceled, recordings and snapshots stored in the bucket will be removed.

AP-Singapore | Select a property or enter a keyword.

Bucket Name	Authorized	Origin Server	Operation
lc[redacted]	Unauthorized	AP-Singapore	Authorize Cancel Authorization
obs-[redacted]	Unauthorized	AP-Singapore	Authorize Cancel Authorization
obs-[redacted]	Unauthorized	AP-Singapore	Authorize Cancel Authorization
obs[redacted]	Authorized	AP-Singapore	Authorize Cancel Authorization
wu[redacted]	Authorized	AP-Singapore	Authorize Cancel Authorization

Total Records: 5 | 10 | 1

----End

Step 3: Configure a Snapshot Template

After OBS authorization is successful, you can configure a snapshot template.

Step 1 Log in to the **Live console**.

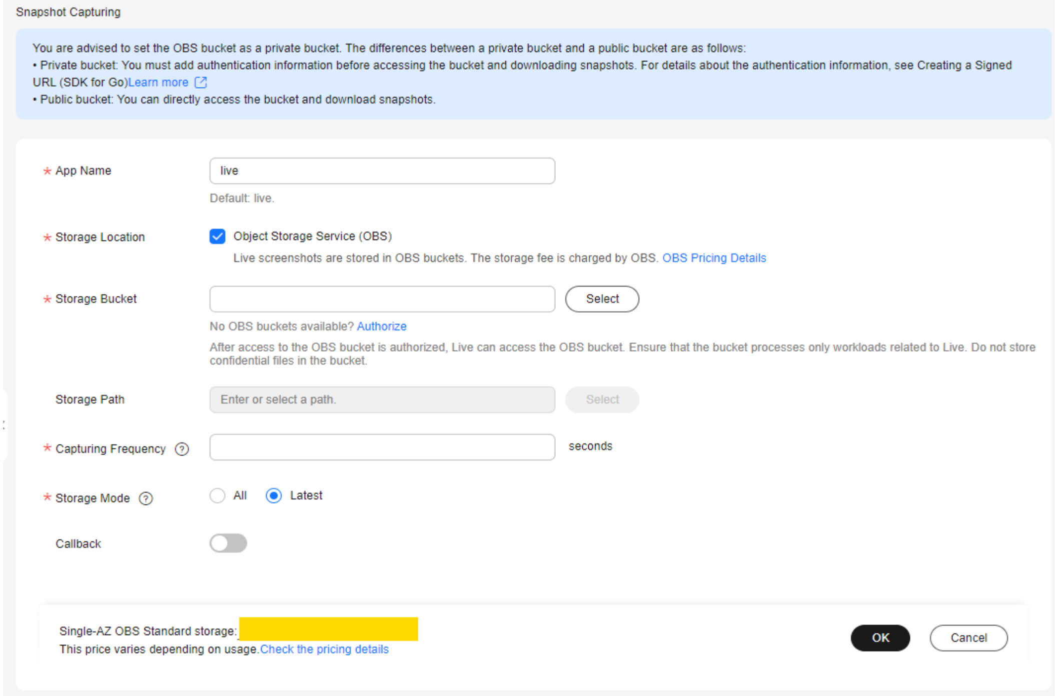
Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Manage** in the **Operation** column of the desired ingest domain name.

Step 4 In the navigation pane, choose **Templates** > **Snapshot Capturing**.

Step 5 Click **Create Snapshot Template**.

Figure 10-9 Creating a snapshot template



Snapshot Capturing

You are advised to set the OBS bucket as a private bucket. The differences between a private bucket and a public bucket are as follows:
• Private bucket: You must add authentication information before accessing the bucket and downloading snapshots. For details about the authentication information, see Creating a Signed URL (SDK for Go)Learn more
• Public bucket: You can directly access the bucket and download snapshots.

* App Name: live
Default: live.

* Storage Location: ☑ Object Storage Service (OBS)
Live screenshots are stored in OBS buckets. The storage fee is charged by OBS. OBS Pricing Details

* Storage Bucket:
No OBS buckets available? Authorize
After access to the OBS bucket is authorized, Live can access the OBS bucket. Ensure that the bucket processes only workloads related to Live. Do not store confidential files in the bucket.

Storage Path: Enter or select a path.

* Capturing Frequency: seconds

* Storage Mode: ○ All ● Latest

Callback

Single-AZ OBS Standard storage: [redacted]
This price varies depending on usage.Check the pricing details

Table 10-5 describes the parameters.

Table 10-5 Template parameters

Parameter	Description
App Name	Application name. The default value is **live**. You can customize the application name. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Storage Location	Live snapshots are stored in OBS.
Storage Bucket	OBS bucket for storing snapshots
Storage Path	OBS bucket path for storing snapshots
Capturing Frequency	Snapshot capturing frequency, in second. Value range: 5 to 3,600
Storage Mode	Snapshot file storage mode. ● **All**: A snapshot file name contains the timestamp. All snapshot files of each stream are stored in OBS. Example: snapshot/{*domain*}/{*app_name*}/{*stream_name*}/{*UnixTimestamp*}.jpg ● **Latest**: A snapshot file name does not contain the timestamp. Only the latest snapshot file of each stream will be saved. A new snapshot file overwrites the previous one. Example: snapshot/{*domain*}/{*app_name*}/{*stream_name*}.jpg

Parameter	Description
Callback	Whether to enable callback
Callback URL	Enter a callback URL when **Callback** is enabled. A callback URL cannot contain message headers or parameters. HTTP and HTTPS (recommended) are supported. Callback messages in JSON format are sent in POST requests to your server through HTTP APIs. For details about a callback message body, see **Callback Message**.
Authentication Key	Authentication key. Configure this parameter only when callback authentication is required. ● A key contains 32 to 128 characters. ● A key can also be automatically generated.

Step 6 Click **OK**.

After a snapshot template is configured, stream push starts. During stream push, snapshots of the livestream are taken based on template settings.

Step 7 Click **Edit** in the **Operation** column to modify template parameters. **App Name** cannot be modified.

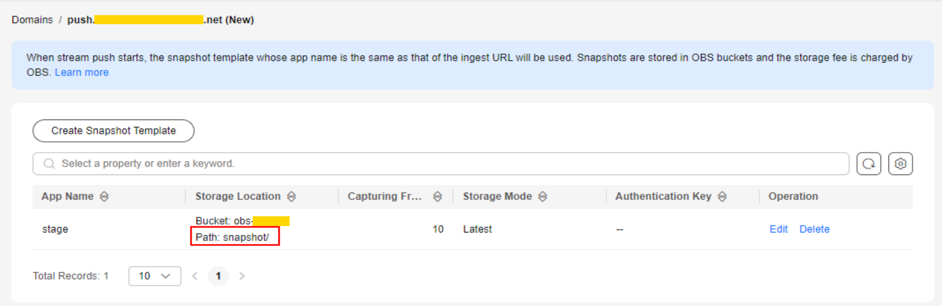
----End

Step 4: View Snapshots

View snapshots in the predefined output path or from a download link in your received callback message.

- Viewing snapshots on the console
  a. Log in to the **Live console**.
  b. In the navigation pane, choose **Domains**.
  c. Click **Manage** in the **Operation** column of the desired ingest domain name.
  d. In the navigation pane, choose **Templates** > **Snapshot Capturing**.
  e. Click the output path in the **Storage Location** column to go to the OBS bucket and view snapshot details.

Figure 10-10 Viewing snapshot details



Domains / push.[redacted].net (New)

When stream push starts, the snapshot template whose app name is the same as that of the ingest URL will be used. Snapshots are stored in OBS buckets and the storage fee is charged by OBS. Learn more

Create Snapshot Template

Select a property or enter a keyword.

App Name	Storage Location	Capturing Fr...	Storage Mode	Authentication Key	Operation
stage	Bucket: obs-[redacted] Path: snapshot/	10	Latest	--	Edit Delete

Total Records: 1 10 < 1 >

You can download and share the snapshots. For details, see **OBS Help Center**.

- Viewing snapshots through a callback message

  If you set a callback URL when **configuring a snapshot template**, then you will receive a message each time a snapshot is generated. **Table 10-6** describes the fields in a callback message.

```
{
    "domain": "play.example.com",
    "app": "live",
    "stream_name": "test001",
    "snapshot_url": "https://xxx.obs.cn-north-4.myhuaweicloud.com:443...",
    "width":"720",
    "height":"1280",
    "obs_addr": {
        "bucket": "xxx",
        "location": "cn-north-4",
        "object": "xxx.jpg"
    },
   "auth_timestamp":1587954140,
    "auth_sign":"4918b1axxxxxxb583cffa119d72513bbc35a989f8569fxxxxxx057646154a04a"
}
```

Table 10-6 Message body

Field	Description
domain	Ingest domain name
app	Application name
stream_name	Stream name
snapshot_url	URL to download snapshots
width	Image width Unit: pixel
height	Image height Unit: pixel
obs_addr	Address of the OBS bucket where snapshots are stored. ● **bucket**: OBS bucket name ● **location**: Region where the OBS bucket is located ● **object**: OBS object path
auth_timestamp	UNIX timestamp when the event notification signature expires. This parameter is carried when an authentication key is configured. The value is a decimal UNIX timestamp, that is, the number of seconds that have elapsed since January 1, 1970 (midnight UTC/GMT). Example: **1592639100** (June 20, 2020 15:45)

Field	Description
auth_sign	Event notification signature. This parameter is carried when an authentication key is configured. `auth_sign = HmacSHA256(domain + app + stream_name + snapshot_url + width + height + obs_addr.bucket + obs_addr.location + obs_addr.object + auth_timestamp,key)` *key* indicates the key used for authentication.

10.5 Stream Status Notifications

You can add a URL on the Live console for receiving messages when stream push starts or ends. The messages are sent as POST requests to your server through an HTTP API. Then your server returns the status code 200 to confirm that the messages have been received.

Notes

After stream status notifications are enabled, you will receive a message each time when a live stream is pushed or disconnected. However, when a stream is disconnected soon after it was pushed, the server may receive the message on stream disconnection before receiving the message on stream pushing due to network transmission latency. In this case, you need to check the Unix timestamp parameter **publish_timestamp** in the message to check whether the stream pushing and stream disconnection are in the same stream pushing event. The timestamps generated in the stream pushing and stream disconnection of the same stream pushing event are the same.

Prerequisites

- You have **added an ingest domain name**.
- You have **configured CNAME records** at your domain names' DNS provider.

Adding a Notification URL

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Manage** in the **Operation** column of the desired ingest domain name.

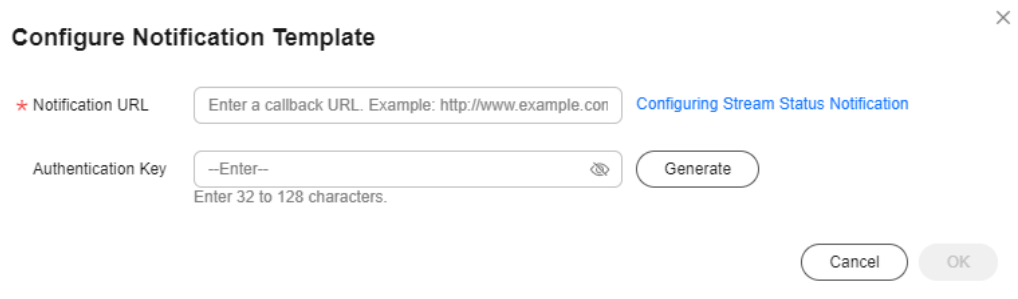
Step 4 In the navigation pane, choose **Template** > **Stream Status Notifications**.

Step 5 Click **Add**. On the displayed dialog box, add a notification URL, as shown in **Figure 10-11**.

NOTE

Only HTTP and HTTPS URLs are supported.

Figure 10-11 Adding a notification URL



Configure Notification Template

* Notification URL: Enter a callback URL. Example: http://www.example.con

Configuring Stream Status Notification

Authentication Key: --Enter--

Enter 32 to 128 characters.

Authentication Key: authentication key. You need to configure this parameter only when notification authentication is required.

- A key contains 32 to 128 characters.
- A key can also be automatically generated.

Step 6 Click **OK**.

When stream pushing starts or ends, you will receive a notification message. For details about the notification message body, see **Callback Example**.

----End

Managing Notification URLs

You can also perform the following operations:

- Editing a notification URL

  Click **Edit** in the **Operation** column to edit the URL or authentication key for receiving stream push messages.

- Deleting a notification URL

  Click **Delete** in the **Operation** column to delete the URL or authentication key for receiving stream push messages.

Callback Example

The following is an example of stream pushing and stream disconnection messages. **Table 10-7** describes the fields in a message body.

```
{
    "domain":"push.example.com",
    "app":"live",
    "stream":"example_stream",
    "user_args":"auth_info=yz1TG0PVN/5isfyrGrRj10gKPCWqSS2X02t6QsRrocH+mEq0gQ0g8k6KhalS84sQ
+kDprFyqI0yajbYiFmUO8e45B7ryaS+MpJBlYkhwnuFLnRiKK/
IXG7.33436b625354564f6e4d4d434f55&cdn=hw",
    "client_ip":"100.111.*.*",
    "node_ip":"112.11.*.*",
    "publish_timestamp":"1587954134",
    "event":"PUBLISH",
    "auth_timestamp":1587954140,
    "auth_sign":"ff3b2bxxx5cfd56e76d72bed4c4aa2dxxxca8c2e46467d205a6417d4fc"
}
```

Table 10-7 Message body

Field	Description
domain	Ingest domain name
app	Application name
stream	Stream name
user_args	Stream pushing parameter
client_ip	IP address of the streaming device
node_ip	IP address of the receiver
publish_timestamp	Unix timestamp. One single timestamp is generated for each stream pushing event.
event	Stream pushing or stream disconnection. Options: ● **PUBLISH**: Stream pushing starts. ● **PUBLISH_DONE**: Stream pushing ends.
auth_timestamp	UNIX timestamp when the event notification signature expires. This parameter is carried when an authentication key is configured. The value is a decimal UNIX timestamp, that is, the number of seconds that have elapsed since January 1, 1970 (midnight UTC/GMT). Example: **1592639100** (June 20, 2020 15:45)
auth_sign	Event notification signature. This parameter is carried when an authentication key is configured. `auth_sign = HmacSHA256 (event + domain + app + stream + auth_timestamp, key)` *key* indicates the key used for authentication.

10.6 HLS

For an ingest domain name, parameters of an HLS livestream, such as **TS Segment Length**, **Segments in Each M3U8 File**, and **Segments in First M3U8 File**, can be modified.

Prerequisites

- You have **added an ingest domain name**.
- You have **configured CNAME records** at your domain names' DNS provider.

Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

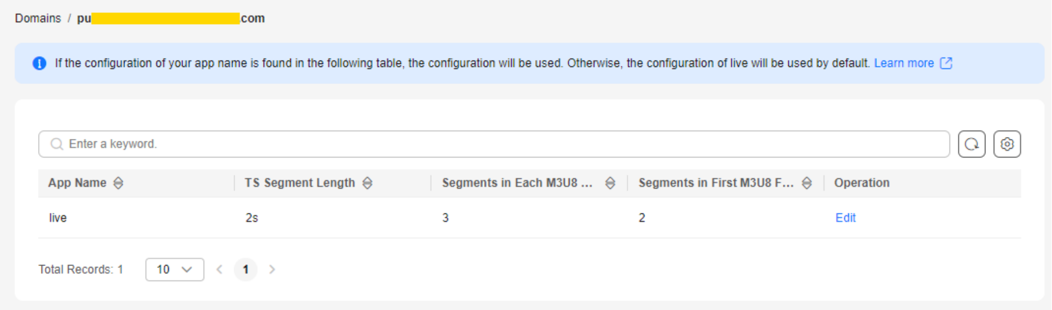
Step 3 Click **Manage** in the **Operation** column of the desired ingest domain name.

Step 4 In the navigation pane, choose **Templates** > **HLS**.

On the page displayed, you can see the configuration of **live**, as shown in **Figure 10-12**.

If you have other applications, they are not displayed by default. You need to **submit a service ticket**to display them on the page.

Figure 10-12 HLS



Domains / pu[redacted]com

If the configuration of your app name is found in the following table, the configuration will be used. Otherwise, the configuration of live will be used by default. Learn more

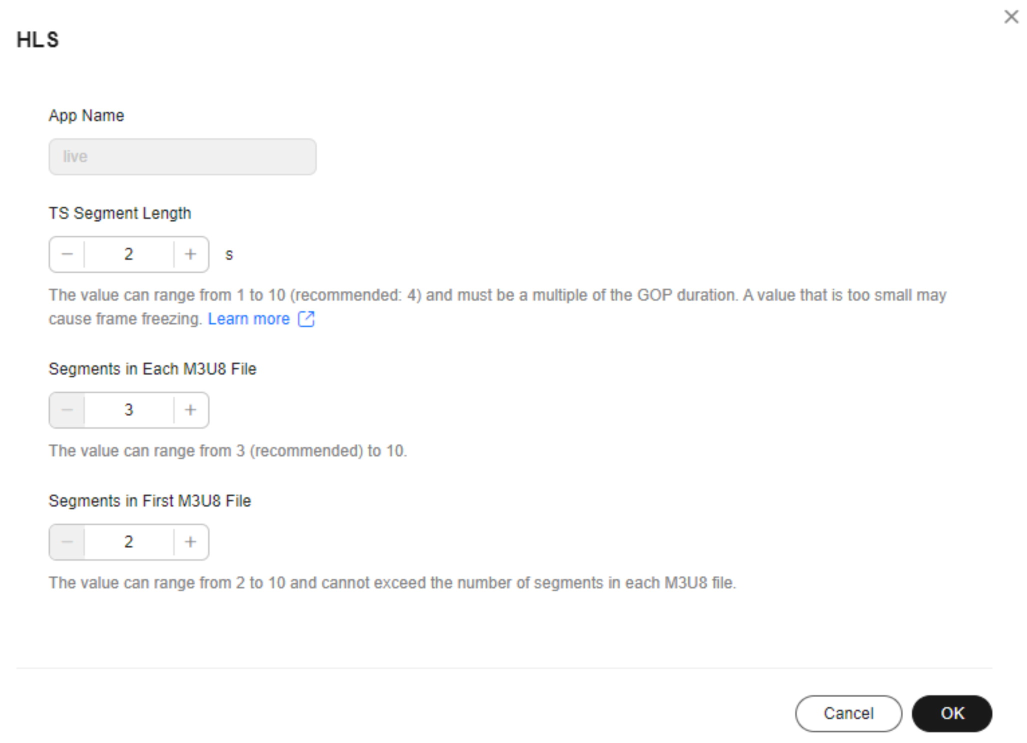
Enter a keyword.

App Name	TS Segment Length	Segments in Each M3U8 ...	Segments in First M3U8 F...	Operation
live	2s	3	2	Edit

Total Records: 1 10 < 1 >

Step 5 Click **Edit** in the **Operation** column. On the page displayed on the right, modify the HLS configuration, as shown in **Figure 10-13**.

Figure 10-13 HLS



HLS

App Name: live

TS Segment Length: 2 s

The value can range from 1 to 10 (recommended: 4) and must be a multiple of the GOP duration. A value that is too small may cause frame freezing. Learn more

Segments in Each M3U8 File: 3

The value can range from 3 (recommended) to 10.

Segments in First M3U8 File: 2

The value can range from 2 to 10 and cannot exceed the number of segments in each M3U8 file.

Table 10-8 describes the parameters.

Table 10-8 HLS configuration

Parameter	Description
App Name	App name of the ingest domain name, which cannot be changed. If the ingestion domain name contains applications other than **live** but no service ticket is submitted to display them, the configuration of **live** will apply to these applications.
TS Segment Length	TS segment length for the HLS. The value must be a multiple of the GOP duration. The value ranges from **1** to **10**, in seconds. A value that is too small may cause frame freezing (recommended: **4**). Default value: **2**
Segments in Each M3U8 File	Number of segments in an M3U8 file. The value ranges from **3** (recommended) to **10**. Default value: **3**
Segments in First M3U8 File	Number of segments in the first M3U8 file. The value cannot exceed the number of segments in each M3U8 file. The value ranges from **2** to **10**. Default value: **2**

Step 6 Click **OK**.

----End

10.7 Stream Authentication

Live provides multiple authentication mechanisms, including referer, URL, and access control list (ACL) validation, to prevent livestreaming resources from being stolen. If multiple authentication mechanisms are configured, livestreaming resources can be accessed only after the access request passes all the authentication mechanisms.

The method of configuring stream authentication is the same as that of configuring playback authentication. For details, see **Referer Validation**, **URL Validation**, and **ACL**.

11 Playback

11.1 Assembling a Streaming URL

After domain names are configured, you can assemble a streaming URL and play the video through the URL. You can also use the **tool** to quickly generate a signed URL of the streaming domain name.

Prerequisites

- The ingest domain name and streaming domain name have been **added** and **associated**.
- You have **configured CNAME records** at your domain names' DNS provider.
- To secure live resources, Live provides URL validation to encrypt and sign the streaming URL. If necessary, configure URL validation and stream the video through the signed URL. For details about how to configure URL validation, see **URL Validation**.
- You can transcode livestreams into video streams with different resolutions and bitrates to meet a broad range of requirements. If necessary, **configure a transcoding template**, and then use the streaming URL to play live video.

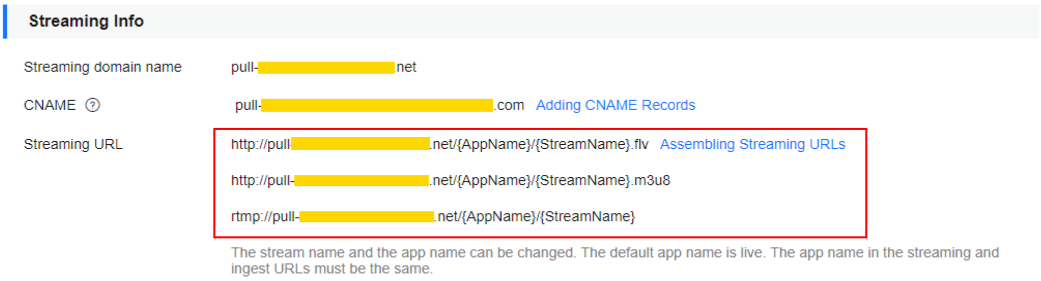
Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Manage** in the **Operation** column of the desired streaming domain name. On the displayed page, you can view streaming information.

Figure 11-1 Viewing the streaming URL



Streaming Info

Streaming domain name pull-[redacted]net

CNAME pull-[redacted].com Adding CNAME Records

Streaming URL

http://pull[redacted].net/{AppName}/{StreamName}.flv Assembling Streaming URLs
http://pull-[redacted].net/{AppName}/{StreamName}.m3u8
rtmp://pull-[redacted].net/{AppName}/{StreamName}

The stream name and the app name can be changed. The default app name is live. The app name in the streaming and ingest URLs must be the same.

- You need to customize **StreamName** to generate a streaming URL. For details, see **Original Streaming URL**.
- If the original streaming URL is used and referer validation is configured, generate a signed streaming URL for the original one by referring to **URL Validation**.
- If the URL of the transcoded stream is used for livestreaming, you need to add ***_transcoding template ID*** to the end of *StreamName* in the original streaming URL to generate a new *StreamName*, and generate new authentication parameters by referring to **URL Validation**. Then you can assemble the streaming URL of the transcoded stream.

----End

Original Streaming URL

Assembling rules

- **Cloud Stream Live**

  You can play FLV, M3U8, and RTMP streams.

  RTMP format: **rtmp://***Streaming domain name***/***AppName***/***StreamName*
  FLV format: **http://***Streaming domain name***/***AppName***/***StreamName***.flv**
  M3U8 format: **http://***Streaming domain name***/***AppName***/***StreamName***.m3u8**

- **LLL**

  You can only play WebRTC streams.

  webrtc://*Streaming domain name*/*AppName*/*StreamName*

Parameters in the example:

- *Streaming domain name* is the one you added on the Live console.
- *AppName*: application name. The default value is **live**. You can customize the application name. Only letters, digits, underscores (_), and hyphens (-) are allowed.
- *StreamName*: livestream name. Multiple livestreams can be created for each application. You can customize the stream name.

Examples

- **Cloud Stream Live**

  If the added streaming domain name is **test-play.example.com**, **AppName** is **livetest**, and **StreamName** is **huawei1**, the assembled streaming URL is:

  ```
  RTMP format: rtmp://test-play.example.com/livetest/huawei1
  FLV format: http://test-play.example.com/livetest/huawei1.flv
  M3U8 format: http://test-play.example.com/livetest/huawei1.m3u8
  ```

- **LLL**

  If the added *streaming domain name* is **test-play.example.com**, *AppName* is **livetest**, and *StreamName* is **huawei1**, the assembled streaming URL is:

  ```
  webrtc://test-play.example.com/livetest/huawei1
  ```

Signed Streaming URL

If URL validation is enabled, you must generate a signed streaming URL based on obtained authentication information and stream your content through the signed URL. For details, see **URL Validation**.

Transcoded Streaming URL

If you have configured **transcoding**, you must assemble a transcoded streaming URL. The URL needs to be set differently when URL validation is enabled or disabled.

Assembling rules

Add _*Transcoding template ID* to the end of the **StreamName** field in the **original streaming URL** and **signed streaming URL**.

- **Cloud Stream Live**

  ```
  RTMP format: rtmp://Streaming domain name/AppName/StreamName_Transcoding template ID
  FLV format: http://Streaming domain name/AppName/StreamName_Transcoding template ID.flv
  M3U8 format: http://Streaming domain name/AppName/StreamName_Transcoding template ID.m3u8
  ```

- **LLL**

  ```
  webrtc://Streaming domain name/AppName/StreamName_Transcoding template ID
  ```

Transcoding template ID: ID of the template used for live transcoding. The ID of a custom transcoding template can be customized. Log in to the **Live console** and choose **Domains** in the navigation pane. On the page displayed, click **Manage** in the **Operation** column of the desired ingest domain name. Then choose **Templates** > **Transcoding** in the navigation pane.

Examples

If the original streaming URL is **http://test-play.example.com/livetest/huawei1.flv** and transcoding template ID is 110,

- The transcoded streaming URL is as follows when URL validation is disabled:
  - **Cloud Stream Live**

    ```
    http://test-play.example.com/livetest/huawei1_110.flv
    ```

  - **LLL**

    ```
    webrtc://test-play.example.com/livetest/huawei1_110
    ```

- The transcoded streaming URL is as follows when URL validation is enabled:
  - **Cloud Stream Live**

    ```
    http://test-play.example.com/livetest/huawei1_110.flv?
    auth_info=z6uwSWUceM2%2FZeDpc2LqjhEFhhXpjQ5IQJhrLoIARQ2%2Bn
    %2BJV4DrzGRqXxWxMLQBU.4439313535383141413245463337 4139
    ```

  - **LLL**

    ```
    webrtc://test-play.example.com/livetest/huawei1_110?
    auth_info=z6uwSWUceM2%2FZeDpc2LqjhEFhhXpjQ5IQJhrLoIARQ2%2Bn
    %2BJV4DrzGRqXxWxMLQBU.4439313535383141413245463337 4139
    ```

  For details about how to generate authentication information, see **Signed Streaming URL**.

11.2 Configuring Stream Delay

You can configure a proper stream delay on the console. Low delay may cause frame freezing.

Notes

- You can configure the stream delay for RTMP and HTTP-FLV streams of the **live** app on the console. To configure the stream delay for other apps, **submit a service ticket**.
- The GOP of the streaming end cannot be greater than the configured delay. The actual delay is influenced by factors including the player's network conditions.
- After the stream delay is modified, you need to push the stream again for the modification to take effect.
- If the stream delay is set to 2s, the playback experience of HLS videos will be affected. For example, the playback will start in seconds. To avoid poor user experience, set a longer stream delay (4s or 6s).
- This function is not recommended for LLL.

Prerequisites

- The ingest domain name and streaming domain name have been **added** and **associated**.
- You have **configured CNAME records** at your domain names' DNS provider.

Procedure

Step 1 Log in to the **Live console**.

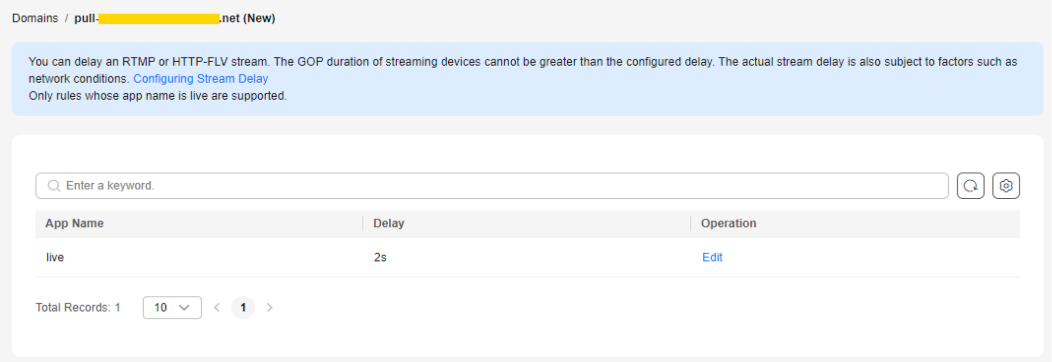
Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Manage** in the **Operation** column of the desired streaming domain name.

Step 4 In the navigation pane, choose **Templates** > **Stream Delay**.

Step 5 Click **Edit** in the **Operation** column.

Figure 11-2 Modifying the stream delay



Domains / pull-[redacted].net (New)

You can delay an RTMP or HTTP-FLV stream. The GOP duration of streaming devices cannot be greater than the configured delay. The actual stream delay is also subject to factors such as network conditions. Configuring Stream Delay
Only rules whose app name is live are supported.

Enter a keyword.

App Name	Delay	Operation
live	2s	Edit

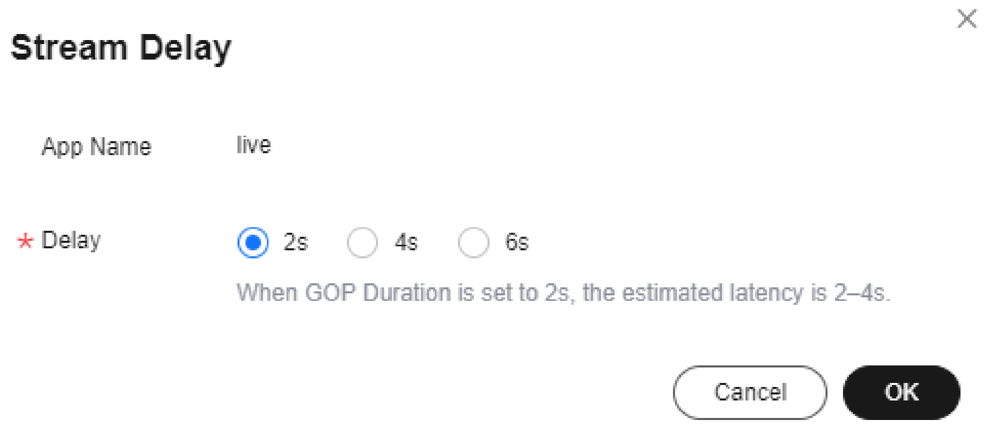
Total Records: 1 10 < 1 >

Step 6 On the page displayed, set **Delay**, as shown in **Figure 11-3**.

The default delay is 2s. You can change it to 4s or 6s. The GOP duration affects the livestream delay, as shown in **Table 11-1**.

Note: The actual livestream delay is also influenced by factors including the player's network conditions.

Figure 11-3 Modifying the delay



Stream Delay

App Name live

* Delay ● 2s ○ 4s ○ 6s

When GOP Duration is set to 2s, the estimated latency is 2–4s.

Table 11-1 Livestream delay

Delay	GOP Duration (1s)	GOP Duration (2s)	GOP Duration (4s)
Estimated delay when **Delay** is set to **2s**	2–3s	2–4s	2–6s
Estimated delay when **Delay** is set to **4s**	4–5s	4–6s	4–8s
Estimated delay when **Delay** is set to **6s**	6–7s	6–8s	6–10s

Step 7 Click **OK**.

----End

11.3 Configuring Origin Pull

By default, a streaming domain name created on Huawei Cloud Live pulls live content from Huawei origin servers. If you want to play live content of non-Huawei origin servers through Huawei Cloud, you can configure an origin address on the Live console so that you can pull live content from your own origin server to a Huawei origin server for accelerated delivery.

Notes

- If you set **Origin Server** to **My origin server (domain name)** or **My origin server (IP address)** for a streaming domain name, livestreams of the ingest domain name associated with this streaming domain name cannot be played, and functions such as transcoding cannot be used.
- The default origin port number is 80 for HTTP and 1935 for RTMP.
- For LLL, ensure that there is no B-frame for origin pull.

Prerequisites

- If **Origin Server** is set to **Huawei origin server**, ensure that you have **added an ingest domain name and a streaming domain name**, **associated the domain names**, and **configured CNAME records** at your domain names' DNS provider.
- If **Origin Server** is set to **My origin server (domain name)** or **My origin server (IP address)**, ensure that you have **added a streaming domain name** and **configured the CNAME record** at your domain names' DNS provider.

Procedure

Step 1 Log in to the **Live console**.

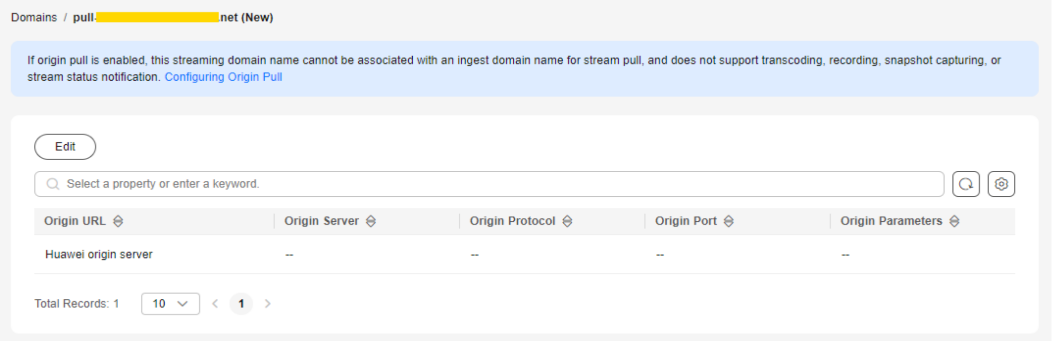
Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Manage** in the **Operation** column of the desired streaming domain name.

Step 4 In the navigation pane, choose **Templates** > **Origin Pull**.

Step 5 View the origin pull configuration.

Figure 11-4 Viewing the origin pull configuration



Domains / pull-[redacted].net (New)

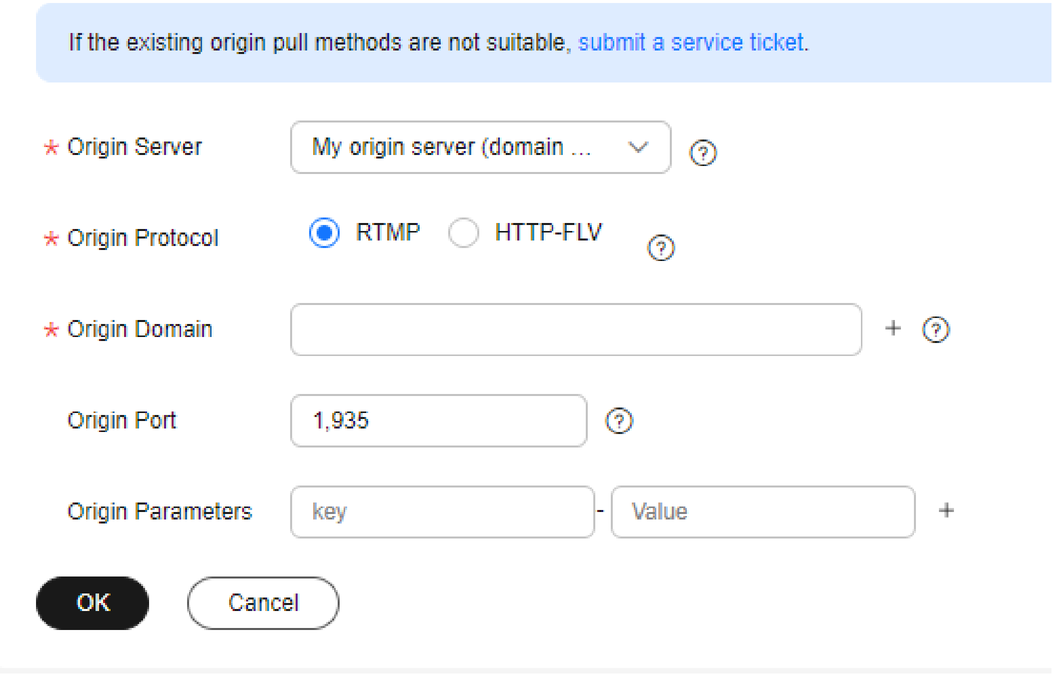
If origin pull is enabled, this streaming domain name cannot be associated with an ingest domain name for stream pull, and does not support transcoding, recording, snapshot capturing, or stream status notification. Configuring Origin Pull

Origin URL	Origin Server	Origin Protocol	Origin Port	Origin Parameters
Huawei origin server	--	--	--	--

Total Records: 1

Step 6 Click **Edit** to modify the origin pull configuration.

Figure 11-5 Configuring origin pull



If the existing origin pull methods are not suitable, submit a service ticket.

* Origin Server: My origin server (domain ...

* Origin Protocol: ● RTMP ○ HTTP-FLV

* Origin Domain:

Origin Port: 1,935

Origin Parameters: key - Value

Table 11-2 describes the parameters.

Table 11-2 Origin pull parameters

Parameter	Description
Origin Server	There are three options: - **Huawei origin server**: pulls livestreams from the Huawei origin server by default - **My origin server (domain name)**: pulls livestreams from your own origin server. You can configure multiple origin domains. - **My origin server (IP address)**: pulls livestreams from your own origin server. You can configure multiple origin IP addresses and one origin domain.
Origin Protocol	Protocol used by Live to pull streams from the origin server. This parameter is used only when **Origin Server** is not **Huawei origin server**. Only RTMP and HTTP-FLV are supported.
Origin IP Address	You can configure a maximum of 10 IP addresses. If an origin pull fails, the system polls origin IP addresses in the configured sequence. This parameter is mandatory when **Origin Server** is set to **My origin server (IP address)**.

Parameter	Description
Origin Domain	Currently, the value can only be a pure domain name, for example, www.example.com. ● This parameter is mandatory when **Origin Server** is set to **My origin server (domain name)**. A maximum of 10 origin domains can be configured. If multiple origin domains are configured, the system polls the domains in the configured sequence when an origin pull fails. ● This parameter is optional when **Origin Server** is set to **My origin server (IP address)**. A maximum of one origin domain can be configured. If an origin domain is configured, both the **HTTP-FLV HOST** header and the **RTMP tcurl** field are set to the origin domain. If there is no origin domain, **HOST** is set to the current IP address.
Origin Port	Customizable. Default values: ● If **Origin Protocol** is set to **HTTP-FLV**, the default value is **80**. ● If **Origin Protocol** is set to **RTMP**, the default value is **1935**.
Origin Parameters	(Optional) When **Origin Server** is set to **My origin server (IP address)** or **My origin server (domain name)**, you can specify the additional parameters carried in the origin URL. Each **key** corresponds to one **value**. You can add multiple pairs. During origin pull, origin parameters are separated using **&**. Example: key1=value1&key2=value2

Step 7 Click **OK**.

Step 8 Assemble a streaming URL for playback.

----End

11.4 HTTPS Secure Acceleration

11.4.1 Configuration Method

You can enable HTTPS secure acceleration to protect your live resources.

Context

Force HTTPS: If a user initiates an HTTP request, the server returns a 302 status code and the request is forcibly redirected to HTTPS.

HTTPS has the following advantages over HTTP:

- HTTPS is a network protocol constructed based on SSL and HTTP for encrypted transmission and identity authentication. It is more secure than HTTP and prevents data from being stolen or changed during transmission to ensure data integrity.
- Key user information is encrypted to prevent session IDs or cookies from being captured by attackers.

Prerequisites

- The ingest domain name and streaming domain name have been **added** and **associated**.
- You have **configured CNAME records** at your domain names' DNS provider.
- An HTTPS certificate is available. If not, buy one in **SSL Certificate Manager (SCM)**.
- The HTTPS certificate format must meet the **requirements**. If your certificate is not in PEM format, **convert the certificate** to the PEM format.

Enabling HTTPS

Step 1 Log in to the **Live console**.

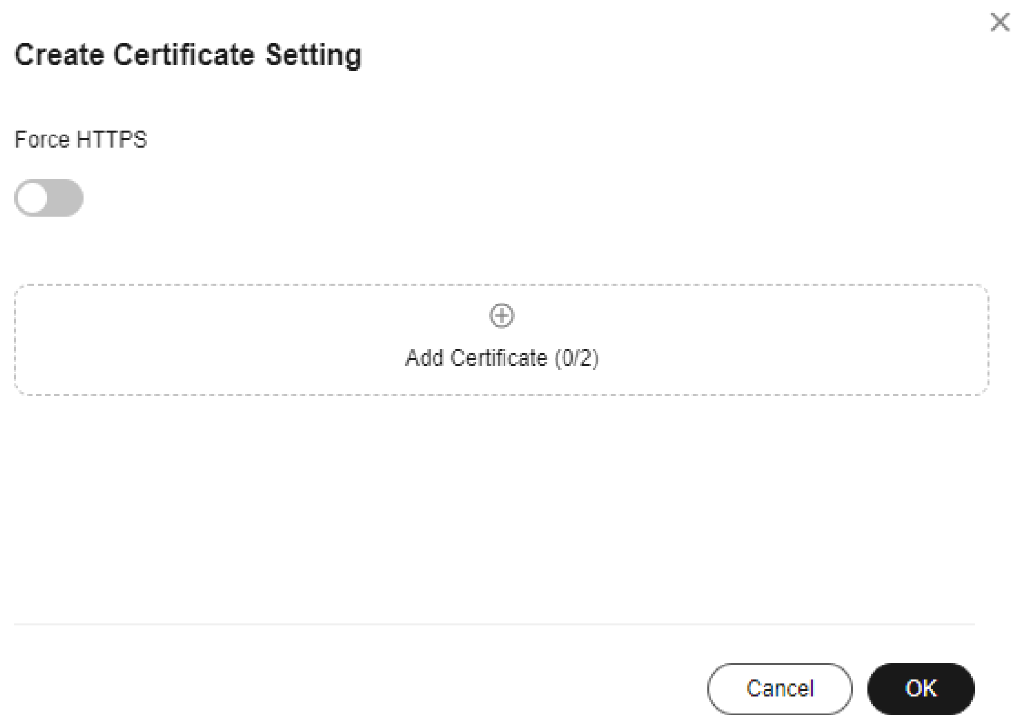
Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Manage** in the **Operation** column of the desired streaming domain name.

Step 4 In the navigation pane, choose **Templates** > **HTTPS Certificates**.

Step 5 Click **Create**. The page of creating certificate settings is displayed, as shown in **Figure 11-6**.

Figure 11-6 Creating certificate settings



Create Certificate Setting

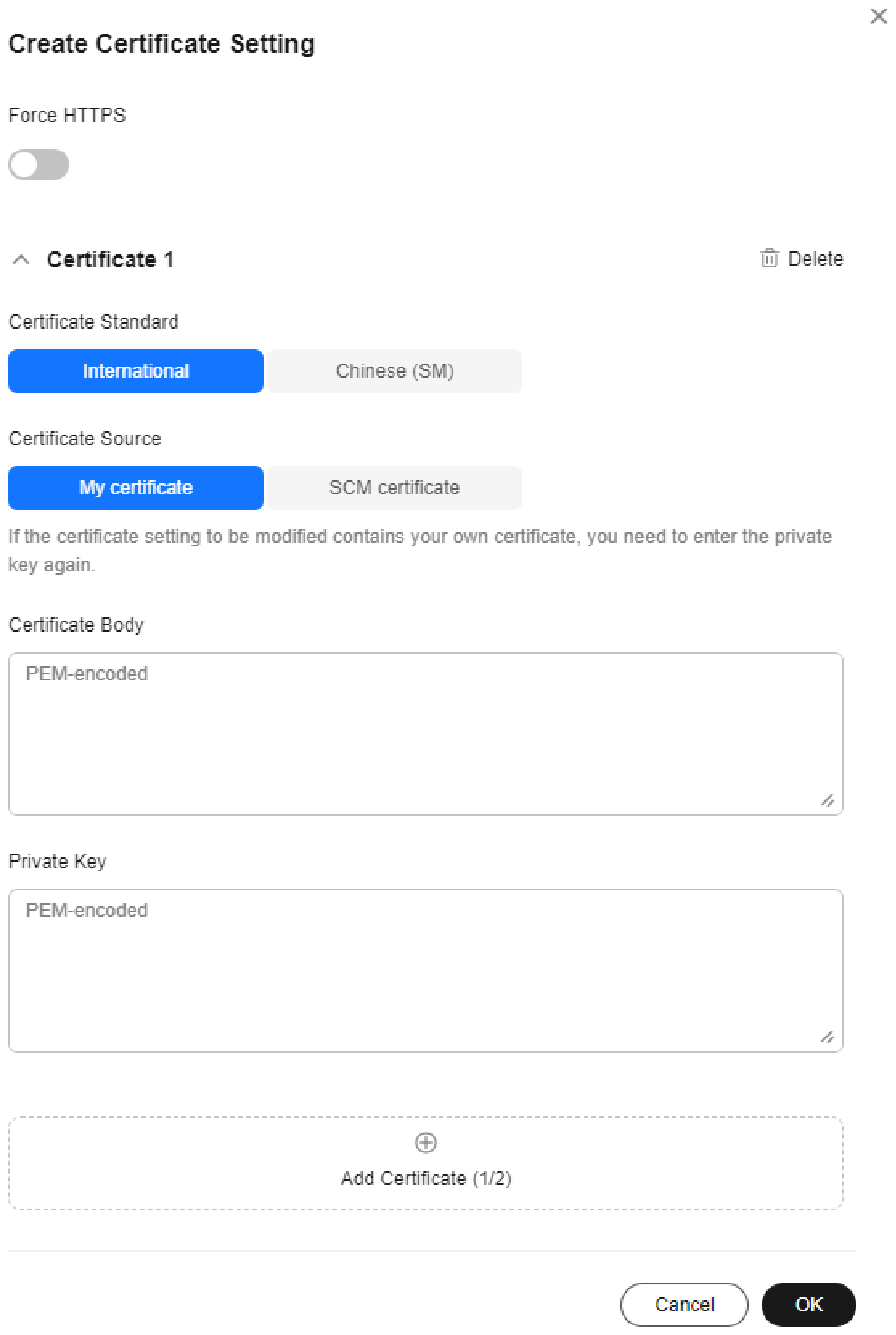
Force HTTPS

Step 6 Click **Add Certificate**. The settings of certificate 1 are displayed, as shown in **Figure 11-7**.

Table 11-3 describes the parameters. You can add a certificate only when:

- There is only one international standard certificate.
- There is only one Chinese (SM) certificate.
- There is one international standard certificate and one Chinese (SM) certificate.

Figure 11-7 Configuring a certificate



Create Certificate Setting

Force HTTPS

Certificate 1

Certificate Standard: International

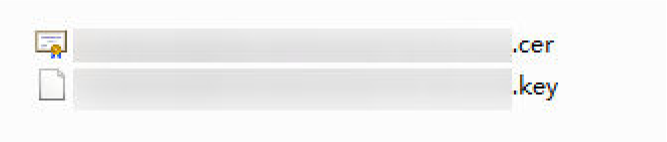
Certificate Source: My certificate

If the certificate setting to be modified contains your own certificate, you need to enter the private key again.

Certificate Body: PEM-encoded

Private Key: PEM-encoded

Table 11-3 Parameters

Parameter	Description
Certificate Standard	Standard of the HTTPS certificate. Options: – **International** – **Chinese (SM)**
Certificate Source	Source of the HTTPS certificate. Options: – **My certificate**: a certificate obtained from a compliant channel – **SCM certificate**: a certificate purchased from Huawei Cloud SCM
International > **My certificate**	Open the obtained certificate file and private key file using a text tool, and copy the certificate body and private key content to the text boxes. Certificates issued by different organizations have the following differences: – If your certificate is issued by the root CA, the certificate is a complete one. Copy the certificate body. **Figure 11-8** HTTPS certificate  – If your certificate is issued by an intermediate CA, the certificate file contains multiple certificates. You need to combine all the certificates into a single certificate.
Chinese (SM) > **My certificate**	
International > **SCM certificate**	Click **Create SCM Certificate** on the right of **Certificate Name** to go to the SCM console and purchase a certificate as prompted. After the certificate is issued, it will be automatically displayed in the **Certificate Name** drop-down list box.
Chinese (SM) > **SCM certificate**	

Step 7 Determine whether to enable **Force HTTPS**.

If this option is enabled, all requests for your website are converted to HTTPS requests.

Step 8 Click **OK**.

Step 9 Verify whether HTTPS secure acceleration has taken effect.

Use an HTTPS streaming URL to play a live video. If the playback is successful, HTTPS secure acceleration has taken effect.

----End

Updating a Certificate

If your certificate has been changed, you need to synchronize the new certificate body to the HTTPS settings. The procedure for updating a certificate is the same as that for **enabling HTTPS**.

If the certificate is your own one, the content in the **Private Key** text box is empty by default to ensure the security and confidentiality of the private key. You need to enter and submit the content again.

11.4.2 HTTPS Certificate Requirements

The HTTPS configuration only supports certificates or private keys in PEM format. The certificate/private key upload requirements vary depending on certificate issuing agencies.

Certificates Issued by Root CA

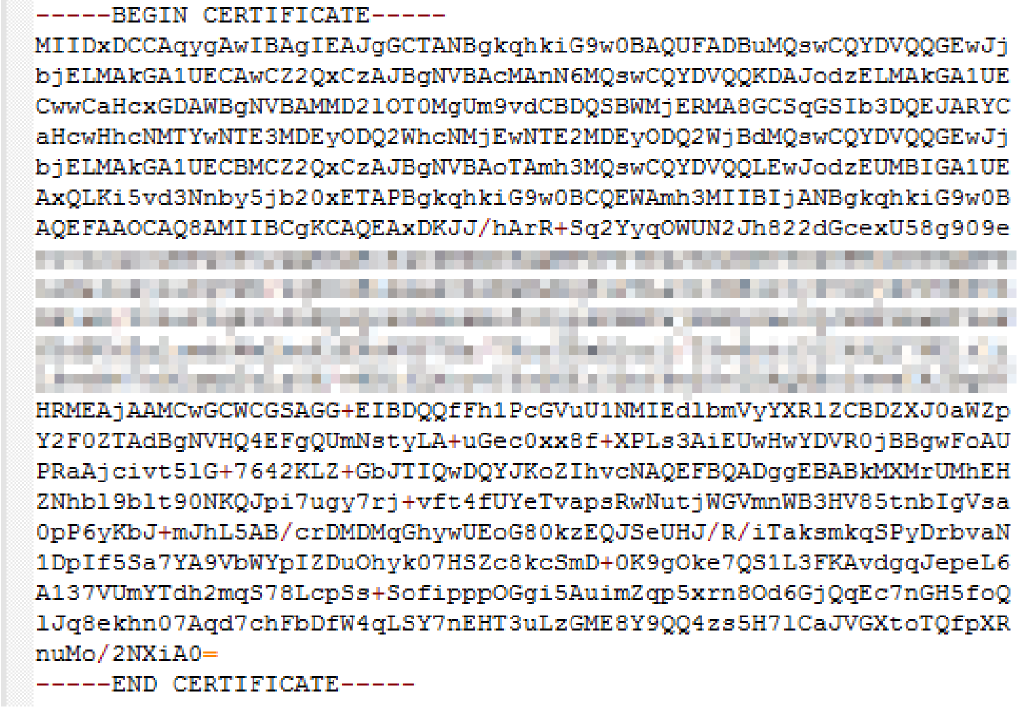
A Certificate issued by Root CA is a complete certificate. You only need to upload the certificate when configuring HTTPS.

Use the text program to open the certificate in the **PEM** format, then you can view the certificate content, as shown in **Figure 11-9**.

A certificate in **PEM** format

- The certificate starts with the **-----BEGIN CERTIFICATE-----** chain and ends with the **-----END CERTIFICATE-----** chain.
- Each line of the certificate content contains 64 characters, but the number of characters in the last line can be smaller than 64.
- No space is allowed in the certificate content.

Figure 11-9 A certificate in **PEM** format



```
-----BEGIN CERTIFICATE-----
MIIDxDCCAqygAwIBAgIEAJgGCTANBgkqhkiG9w0BAQUFADBuMQswCQYDVQQGEwJj
bjELMAkGA1UECAwCZ2QxCzAJBgNVBAcMAnN6MQswCQYDVQQKDAJodzELMAkGA1UE
CwwCaHcxGDAWBgNVBAMMD2l0T0MgUm9vdCBDQSBWMjERMA8GCSqGSIb3DQEJARYC
aHcwHhcNMTYwNTE3MDEyODQ2WhcNMjEwNTE2MDEyODQ2WjBdMQswCQYDVQQGEwJj
bjELMAkGA1UECBMCZ2QxCzAJBgNVBAoTAmh3MQswCQYDVQQLEwJodzEUMBIGA1UE
AxQLKi5vd3Nnby5jb20xETAPBgkqhkiG9w0BCQEWAmh3MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAxDKJJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909e
[redacted]
HRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZp
Y2F0ZTAdBgNVHQ4EFgQUmNstyLA+uGec0xx8f+XPLs3AiEUwHwYDVR0jBBgwFoAU
PRaAjcivt5lG+7642KLZ+GbJTIQwDQYJKoZIhvcNAQEFBQADggEBABkMXMrUMhEH
ZNhbl9blt90NKQJpi7ugy7rj+vft4fUYeTvapsRwNutjWGVmnWB3HV85tnbIgVsa
0pP6yKbJ+mJhL5AB/crDMDMqGhywUEoG80kzEQJSeUHJ/R/iTaksmkqSPyDrbvaN
1DpIf5Sa7YA9VbWYpIZDuOhyk07HSZc8kcSmD+0K9gOke7QS1L3FKAvdgqJepeL6
A137VUmYTdh2mqS78LcpSs+SofipppOGgi5AuimZqp5xrn8Od6GjQqEc7nGH5foQ
lJq8ekhn07Aqd7chFbDfW4qLSY7nEHT3uLzGME8Y9QQ4zs5H7lCaJVGXtoTQfpXR
nuMo/2NXiA0=
-----END CERTIFICATE-----
```

Certificates Issued by Intermediate CAs

The certificate file issued by an intermediate agency contains several certificates. You need to combine the certificates into an integral one, and upload it when configuring HTTPS security acceleration. A combined certificate is shown as **Figure 11-10**.

Use the text program to open all the certificates in the **PEM** format. Put the server certificate on the top and then the intermediate certificate. Generally, an instruction will be issued together with the certificate. Be aware of the rules in the instruction. The general rules are as follows:

- There are no lines between certificates.
- The formats of certificate chains are as follows:

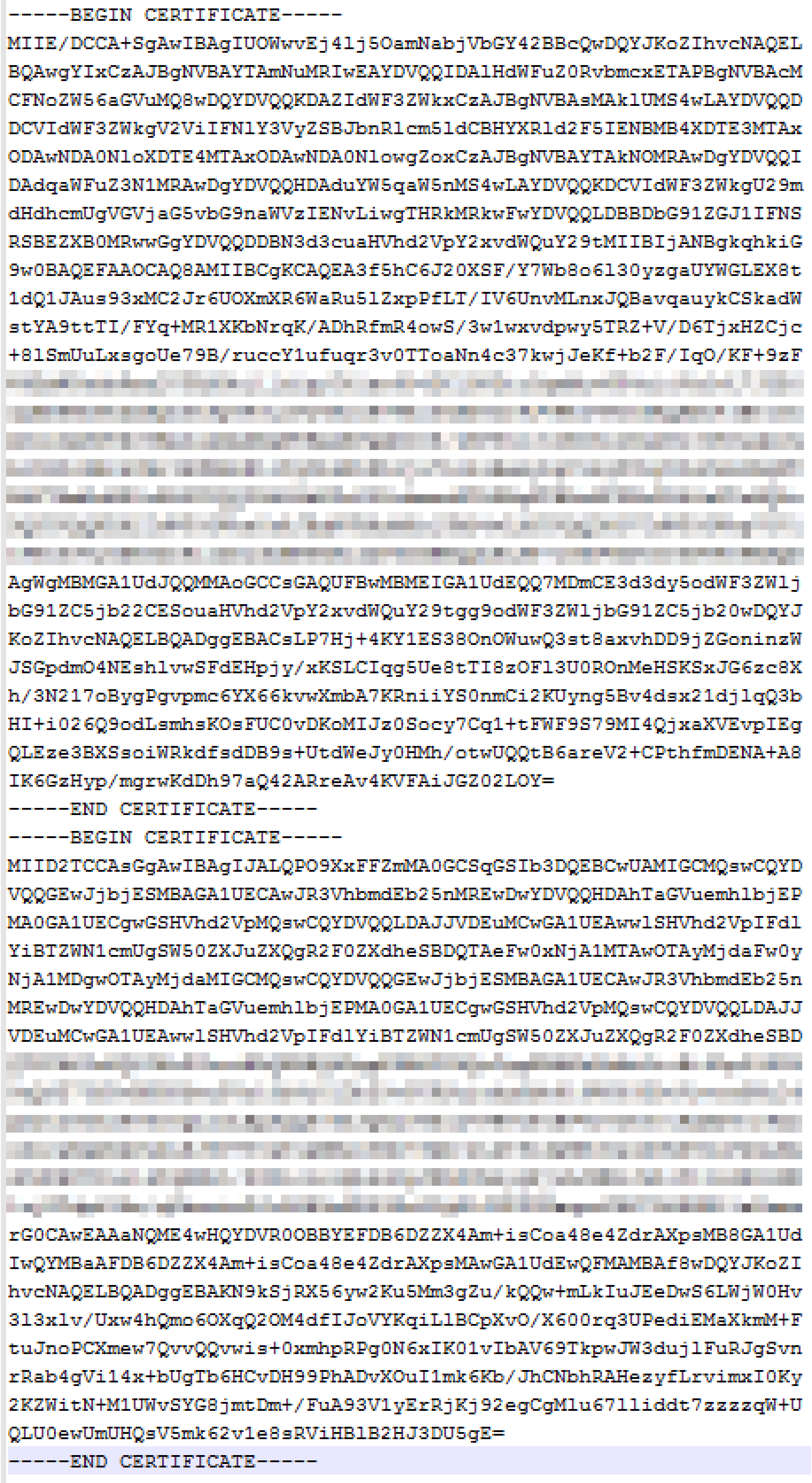
  -----BEGIN CERTIFICATE-----

  -----END CERTIFICATE-----

  -----BEGIN CERTIFICATE-----

  -----END CERTIFICATE-----

Figure 11-10 A combined certificate



```
-----BEGIN CERTIFICATE-----
MIIE/DCCA+SgAwIBAgIUOWwvEj41j5OamNabjVbGY42BBcQwDQYJKoZIhvcNAQEL
BQAwgYIxCzAJBgNVBAYTAmNuMRIwEAYDVQQIDA1HdWFuZ0RvbmcxETAPBgNVBAcM
CFNoZW56aGVuMQ8wDQYDVQQKDAZIdWF3ZWkxCzAJBgNVBAsMAk1UMS4wLAYDVQQD
DCVIdWF3ZWkgV2ViIFN1Y3VyZSBJbnR1cm51dCBHYXR1d2F5IENBMB4XDTE3MTAx
ODAwNDA0NloXDTE4MTAxODAwNDA0NlowgZoxCzAJBgNVBAYTAkNOMRAwDgYDVQQI
DAdqaWFuZ3N1MRAwDgYDVQQHDAduYW5qaW5nMS4wLAYDVQQKDCVIdWF3ZWkgU29m
dHdhcmUgVGVjaG5vbG9naWVzIENvLiwgTHRkMRkwFwYDVQQLDBBDbG91ZGJ1IFNS
RSBEZXB0MRwwGgYDVQQDDBN3d3cuaHVhd2VpY2xvdWQuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3f5hC6J20XSF/Y7Wb8o6l30yzgaUYWGLEX8t
1dQ1JAus93xMC2Jr6UOXmXR6WaRu5lZxpPfLT/IV6UnvMLnxJQBavqauykCSkadW
stYA9ttTI/FYq+MR1XKbNrqK/ADhRfmR4owS/3w1wxvdpwy5TRZ+V/D6TjxHZCjc
+8lSmUuLxsgoUe79B/ruccY1ufuqr3v0TToaNn4c37kwjJeKf+b2F/IqO/KF+9zF
[redacted]
AgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMEIGA1UdEQQ7MDmCE3d3dy5odWF3ZW1j
bG91ZC5jb22CESouaHVhd2VpY2xvdWQuY29tgg9odWF3ZW1jbG91ZC5jb20wDQYJ
KoZIhvcNAQELBQADggEBACsLP7Hj+4KY1ES38OnOWuwQ3st8axvhDD9jZGoninzW
JSGpdmO4NEshlvwSFdEHpjy/xKSLCIqg5Ue8tTI8zOF13U0ROnMeHSKSxJG6zc8X
h/3N217oBygPgvpmc6YX66kvwXmbA7KRniiYS0nmCi2KUyng5Bv4dsx21djlqQ3b
HI+i026Q9odLsmhsKOsFUC0vDKoMIJz0Socy7Cq1+tFWF9S79MI4QjxaXVEvpIEg
QLEze3BXSsoiWRkdfsdDB9s+UtdWeJy0HMh/otwUQQtB6areV2+CPthfmDENA+A8
IK6GzHyp/mgrwKdDh97aQ42ARreAv4KVFAiJGZ02LOY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID2TCCAsGgAwIBAgIJALQPO9XxFFZmMA0GCSqGSIb3DQEBCwUAMIGCMQswCQYD
VQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25nMREwDwYDVQQHDAhTaGVuemhlbjEP
MA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDAJJVDEuMCwGA1UEAww1SHVhd2VpIFdl
YiBTZWN1cmUgSW50ZXJuZXQgR2F0ZXdheSBDQTAeFw0xNjA1MTAwOTAyMjdaFw0y
NjA1MDgwOTAyMjdaMIGCMQswCQYDVQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25n
MREwDwYDVQQHDAhTaGVuemhlbjEPMA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDAJJ
VDEuMCwGA1UEAww1SHVhd2VpIFdlYiBTZWN1cmUgSW50ZXJuZXQgR2F0ZXdheSBD
[redacted]
rG0CAwEAAaNQME4wHQYDVR0OBBYEFDB6DZZX4Am+isCoa48e4ZdrAXpsMB8GA1Ud
IwQYMBaAFDB6DZZX4Am+isCoa48e4ZdrAXpsMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAKN9kSjRX56yw2Ku5Mm3gZu/kQQw+mLkIuJEeDwS6LWjW0Hv
3l3xlv/Uxw4hQmo6OXqQ2OM4dfIJoVYKqiLlBCpXvO/X600rq3UPediEMaXkmM+F
tuJnoPCXmew7QvvQQvwis+0xmhpRPg0N6xIK01vIbAV69TkpwJW3dujlFuRJgSvn
rRab4gVi14x+bUgTb6HCvDH99PhADvXOuI1mk6Kb/JhCNbhRAHezyfLrvimxI0Ky
2KZWitN+M1UWvSYG8jmtDm+/FuA93V1yErRjKj92egCgMlu67lliddt7zzzzqW+U
QLU0ewUmUHQsV5mk62v1e8sRViHB1B2HJ3DU5gE=
-----END CERTIFICATE-----
```

RSA Private Key

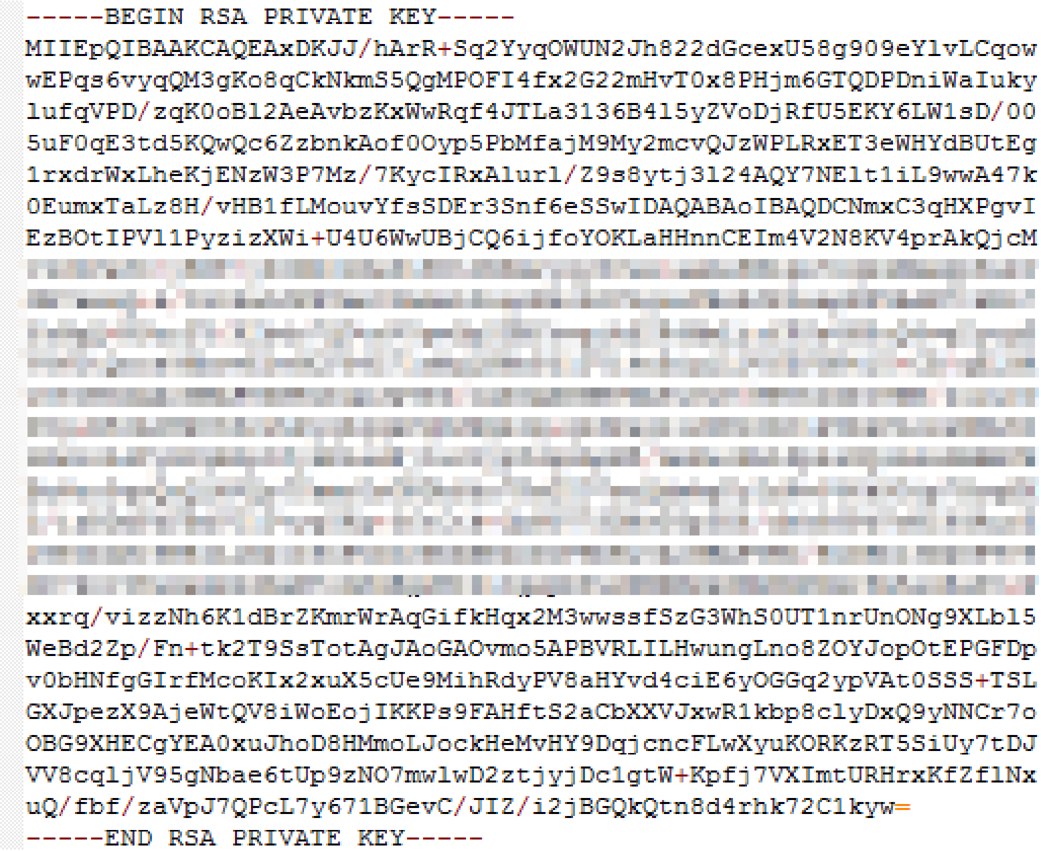
PEM files can contain certificates or private keys. If a PEM file contains only private keys, the file suffix may be replaced by KEY.

Use the text program to open the private key file in the PEM or KEY format, then you can view the private key content, as shown in **Figure 11-11**.

Content of an RSA private key:

- The private key starts with the **-----BEGIN RSA PRIVATE KEY-----** chain and ends with the **-----END RSA PRIVATE KEY-----** chain.
- Each line of the private key content contains 64 characters, but the number of characters in the last line can be smaller than 64.
- No space is allowed in the private key content.

Figure 11-11 An RSA private key



```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAxDKJJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909eYlvLCqow
wEPqs6vyqQM3gKo8qCkNkmS5QgMPOFI4fx2G22mHvT0x8PHjm6GTQDPDniWaIuky
lufqVPD/zqK0oBl2AeAvbzKxWwRqf4JTLa3136B415yZVoDjRfU5EKY6LW1sD/00
5uF0qE3td5KQwQc6ZzbnkAof0Oyp5PbMfajM9My2mcvQJzWPLRxET3eWHYdBUtEg
1rxdrWxLheKjENzW3P7Mz/7KycIRxAlurl/Z9s8ytj3124AQY7NE1t1iL9wwA47k
0EumxTaLz8H/vHB1fLMouvYfsSDEr3Snf6eSSwIDAQABAoIBAQDCNmxC3qHXPgvI
EzBOtIPVl1PyzizXWi+U4U6WwUBjCQ6ijfoYOKLaHHnnCEIm4V2N8KV4prAkQjcM
[redacted]
xxrq/vizzNh6K1dBrZKmrWrAqGifkHqx2M3wwssfSzG3WhS0UT1nrUnONg9XLbl5
WeBd2Zp/Fn+tk2T9SsTotAgJAoGAOvmo5APBVRLILHwungLno8ZOYJopOtEPGFDp
v0bHNfgGIrfMcoKIx2xuX5cUe9MihRdyPV8aHYvd4ciE6yOGGq2ypVAt0SSS+TSL
GXJpezX9AjeWtQV8iWoEojIKKPs9FAHftS2aCbXXVJxwR1kbp8clyDxQ9yNNCr7o
OBG9XHECgYEA0xuJhoD8HMmoLJockHeMvHY9DqjcncFLwXyuKORKzRT5SiUy7tDJ
VV8cqljV95gNbae6tUp9zNO7mwlwD2ztjyjDc1gtW+Kpfj7VXImtURHrxKfZflNx
uQ/fbf/zaVpJ7QPcL7y671BGevC/JIZ/i2jBGQkQtn8d4rhk72C1kyw=
-----END RSA PRIVATE KEY-----
```

If the certificate chain of a private key file contains the following information: **-----BEGIN PRIVATE KEY-----** and **-----END PRIVATE KEY-----**, or **-----BEGIN ENCRYPTED PRIVATE KEY-----** and **-----END ENCRYPTED PRIVATE KEY-----**, you need to use the OpenSSL tool to run the following command to convert the format.

```
openssl rsa -in old_key.pem -out new_key.pem
```

Format Conversion

The HTTPS configuration only supports certificates or private keys in **PEM** format. It is recommended that **OpenSSL** be used to convert certificates in other formats into the **PEM** format. The following examples illustrate some popular converting methods.

In the following examples, the name of certificates before conversion is **old_certificate** by default, and that of private keys before transformation is **old_key** by default. The new certificate and private key names are **new_certificate** and **new_key** respectively.

- **Converting DER to PEM**
  ```
  openssl x509 -inform der -in old_certificate.cer -out new_certificate.pem
  openssl rsa -inform DER -outform pem -in old_key.der -out new_key.pem
  ```
- **Converting P7B to PEM**
  ```
  openssl pkcs7 -print_certs -in old_certificate.p7b -out new_certificate.cer
  ```
- **Converting PFX to PEM**
  ```
  openssl pkcs12 -in old_certificat.pfx -nokeys -out new_certificate.pem
  openssl pkcs12 -in old_certificat.pfx -nocerts -out new_key.pem
  ```

To convert a PKCS8 private key to a PKCS1 one, run the following command:

```
openssl rsa -in old_certificat.pem -out pkcs1.pem
```

11.5 Playback Authentication

11.5.1 Overview

Live provides referer validation, URL validation, and ACL to identify and filter out malicious visitors. Only visitors that meet the rules can use Live.

URL validation protects live resources from unauthorized download and theft. Referer validation uses referer blacklists/whitelists to prevent hotlinking. However, because the referer content can be forged, referer validation cannot well protect live resources. Therefore, you are advised to use URL validation. **Table 11-4** shows the authentication mechanism of the Live service.

Table 11-4 Authentication mechanism

Function	Description	Configuration
Referer validation	You can configure the referer blacklist and whitelist to identify and filter out malicious visitors.	For details, see **Referer Validation**
URL validation	You can configure a key and validate the URL to protect live resources.	For details, see **URL Validation**.

Function	Description	Configuration
ACL	You can configure an IP address blacklist and whitelist to identify and filter out malicious visitors.	For details, see **ACL**.

11.5.2 Referer Validation

Referer validation allows you to control access sources based on the referer field carried in an HTTP request. CDN allows or rejects playback requests based on the configured blacklist or whitelist.

Notes

- This function is optional and is disabled by default.
- Whitelisting and blacklisting cannot be used simultaneously.
- A maximum of 100 domain names can be added to a blacklist or whitelist.
- Domain names added to a blacklist or whitelist are matched using regular expressions. For example, if you add **^http://test.*com$** to a blacklist or whitelist, **http://test.example.com** and **http://test.example01.com** are also matched.

Prerequisites

- The ingest domain name and streaming domain name have been **added** and **associated**.
- You have **configured CNAME records** at your domain names' DNS provider.

Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

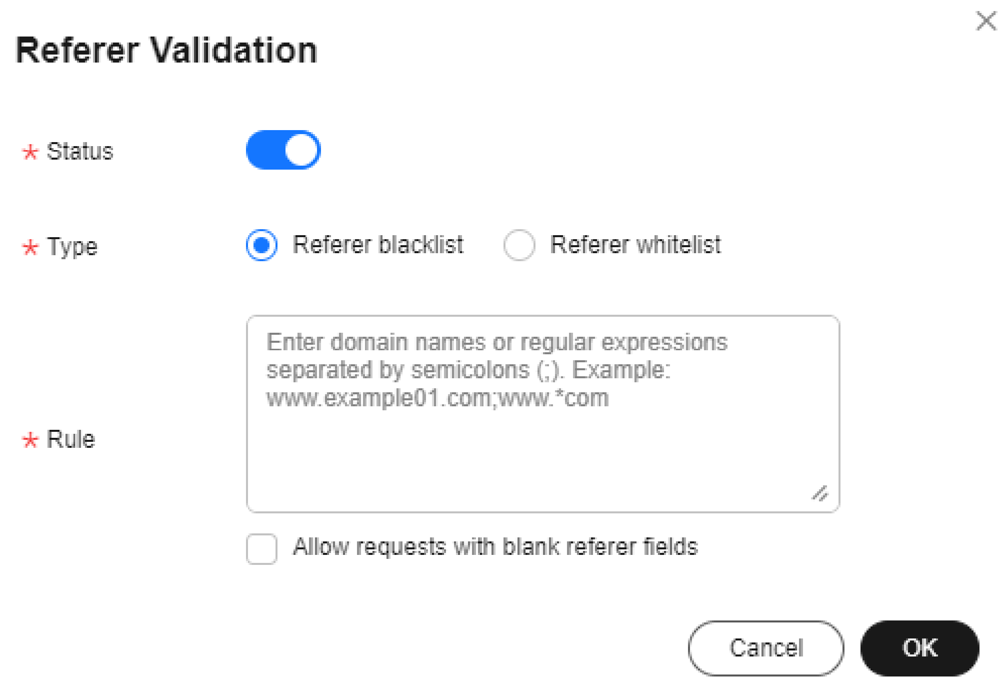
Step 3 Click **Manage** in the **Operation** column of the desired streaming domain name.

Step 4 In the navigation pane, choose **Basic Settings** > **Access Control**.

Step 5 Choose **Referer Validation**. The **Referer Validation** dialog box is displayed.

Step 6 Toggle on the switch and configure related parameters.

Figure 11-12 Configuring referer validation



Referer Validation

* Status

* Type ● Referer blacklist ○ Referer whitelist

* Rule Enter domain names or regular expressions separated by semicolons (;). Example: www.example01.com;www.*com

□ Allow requests with blank referer fields

Table 11-5 describes the parameters.

Table 11-5 Parameter description

Parameter	Description
Type	The blacklist and whitelist are supported. ● **Referer blacklist** allows all domains access to CDN except for the domains added to the blacklist. ● **Referer whitelist** denies all domains access to CDN except for the domains added to the whitelist. You can set whether to allow requests with empty referer fields, that is, whether to allow access through the browser address bar.
Rule	Domain name in the blacklist or whitelist. ● You can input 1 to 100 domain names. Use semicolons (;) to separate domain names. ● Domain names are matched using regular expressions. If **^http://test.*com$** is entered, **http://test.example.com** and **http://test.example01.com** are also matched.

Step 7 Click **OK**.

----End

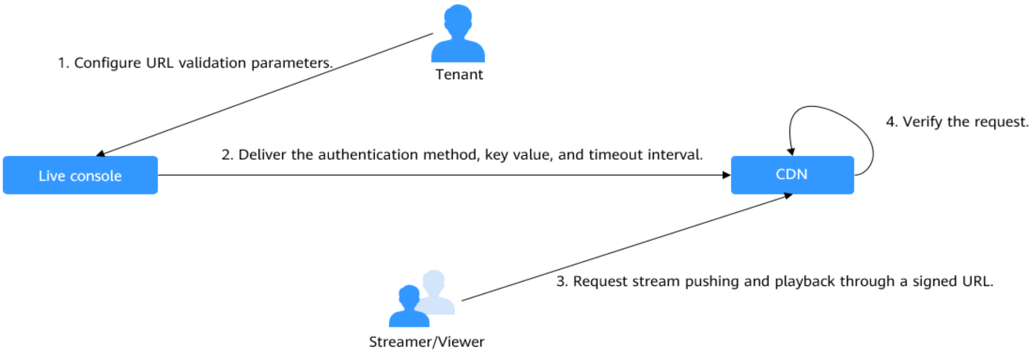
11.5.3 URL Validation

To prevent live resources from being stolen, you can configure URL validation to add authentication information to the end of the original ingest or streaming URL. When a streamer starts live streaming or a viewer requests playback, CDN verifies encrypted information in a URL. Only the requests that pass the verification are responded, and other illegitimate requests are rejected.

If you need to customize other validation rules, **submit a service ticket** to contact Huawei Cloud technical support.

Working Principle

Figure 11-13 URL validation working principles


1. Configure URL validation parameters.
Tenant
4. Verify the request.
2. Deliver the authentication method, key value, and timeout interval.
Live console
CDN
3. Request stream pushing and playback through a signed URL.
Streamer/Viewer

The process is as follows:

1. A tenant enables URL validation on the Live console and configures the authentication method, the key, and timeout interval.
2. The Live service delivers the configured authentication method, key value, and timeout interval to a CDN node.
3. The streamer or viewer requests CDN to push streams or play video through a signed ingest/streaming URL.
4. CDN verifies the request based on authentication information carried in the URL. Only requests that pass the verification are allowed.

Notes

- This function is optional and is disabled by default. After this function is enabled, the original URLs cannot be used. New signed URLs must be generated based on rules.
- Use different keys for streaming authentication and playback authentication to enhance security. If a signed URL expires or the signature fails to be authenticated, the livestream fails to be played and the message "403 Forbidden" is returned.
- For persistent connection services such as RTMP and FLV, the server verifies the validation parameters only when receiving a user request. Once verified, the content can be played continuously.
- For HLS services, users keep sending requests that contain the same validation parameters after content is played. Once the validation parameters

expire, the server rejects the access request because the verification fails, which will interrupt the playback.

For such services, you need to set a proper authentication expiration time to prevent playback failures. For example, if the estimated HLS playback lasts less than 1 hour each time, you can set the expiration time to 3600 seconds.

Prerequisites

- The ingest domain name and streaming domain name have been **added** and **associated**.
- You have **configured CNAME records** at your domain names' DNS provider.

Enabling URL Validation

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

Step 3 Click **Manage** in the **Operation** column of the desired domain name.

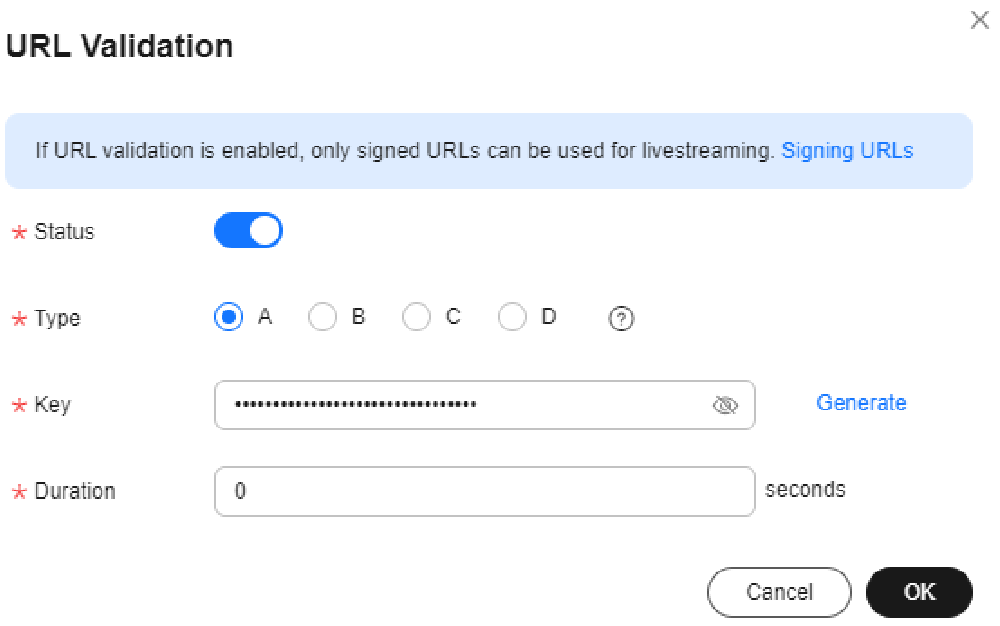
Step 4 In the navigation pane, choose **Basic Settings** > **Access Control**.

Step 5 Choose **URL Validation**.

The **URL Validation** dialog box is displayed.

Step 6 Toggle on the switch and configure related parameters.

Figure 11-14 Configuring URL validation



URL Validation

If URL validation is enabled, only signed URLs can be used for livestreaming. Signing URLs

* Status: on

* Type: ● A ○ B ○ C ○ D

* Key: ••••••••••••••••••••••••••••••••••

* Duration: 0 seconds

Table 11-6 URL validation parameters

Parameter	Description
Method	You can use signing method A, B, C, or D to calculate a signed string. Signing methods A and B: The Message Digest algorithm 5 (MD5) is used. For details, see **Signing Method A** and **Signing Method B**. Signing method C: A symmetric encryption algorithm is used. For details, see **Signing Method C**. Signing method D: The HMAC-SHA256 algorithm is used. For details, see **Signing Method D**. **NOTE** Signing methods A, B, and C have security risks. Signing method D is more secure and recommended.
Key	Authentication key. ● You can customize a key. A key consists of 32 characters. Only letters and digits are allowed. ● A key can also be automatically generated.
Duration	Timeout interval of URL authentication information, that is, the maximum difference between the request time carried in authentication information and the time when Live receives the request. This parameter is used to check whether an ingest URL or streaming URL expires. The unit is second. The value ranges from 1 minute to 30 days. **NOTE** ● For persistent connection services such as RTMP and FLV, the server verifies the validation parameters only when receiving a user request. Once verified, the content can be played continuously. ● For HLS services, users keep sending requests that contain the same validation parameters after content is played. Once the validation parameters expire, the server rejects the access request because the verification fails, which will interrupt the playback. For such services, you need to set a proper authentication expiration time to prevent playback failures. For example, if the estimated HLS playback lasts less than 1 hour each time, you can set the expiration time to 3600 seconds.

Step 7 Click **OK**.

Step 8 Obtain a signed URL in either of the following ways.

- Manually generate a signed URL based on the configured authentication type. For details, see **Signing Method A**, **Signing Method B**, **Signing Method C**, and **Signing Method D**.
- Use the tool to automatically generate a signed URL. For details, see **Signed URL Generation Tool**.

Step 9 Verify whether URL validation has taken effect.

Use a third-party livestreaming tool to verify the signed ingest URL and streaming URL. If the original ingest URL and streaming URL cannot be used but the signed ingest URL and streaming URL can, URL validation has taken effect.

----End

Signing Method A

A signed string is calculated based on the **Key**, **timestamp**, **rand** (random), **uid** (set to **0**), and URL.

Signed URL format:

```
Original URL?auth_key={timestamp}-{rand}-{uid}-{md5hash}
```

Formula for calculating **md5hash** is:

```
sstring = "{URI}-{Timestamp}-{rand}-{uid}-{Key}"
HashValue = md5sum(sstring)
```

Table 11-7 Authentication fields

Field	Description
timestamp	Start time of a valid request. The value is the total number of seconds that have elapsed since 00:00:00 January 1, 1970. It is a decimal or hexadecimal integer. Example: **1592639100** (June 20, 2020 15:45)
Duration	How long a signed URL remains effective. If the validity period is set to 1800s, users can access the streaming URL within 1800s since the time indicated by **timestamp**. Authentication fails and the URL is inaccessible if users access the streaming URL 1800s later. For example, if the access time is 00:00:00 (GMT +08:00) on June 30, 2020, the URL expires at 00:30:00 (GMT+08:00) on June 30, 2020.
rand	Random number. The recommended value is a UUID, which cannot contain hyphens (-). Example: 477b3bbc253f467b8def6711128c7bec
uid	User ID. This parameter is not used now. Set it to **0**.

md5hash	A string of 32 characters calculated using the MD5 algorithm. The string consists of digits (0 to 9) and lowercase letters.
	sstring = "{URI}-{Timestamp}-{rand}-{uid}-{Key}"
	HashValue = md5sum(sstring)

URI	Path from the domain name to the end in the original URL ● **Cloud Stream Live** Example: /livetest/huawei1.flv ● **LLL** Example: /livetest/huawei1.sdp

Field	Description
Key	Key value set on the console. For details, see **URL Validation**

Signed URL example:

- **Cloud Stream Live**

  Generating a signed streaming URL is used as an example.

  ```
  Original URL: http://test-play.example.com/livetest/huawei1.flv
  timestamp: 1592639100
  Validity period: 1800s
  Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
  rand: 477b3bbc253f467b8def6711128c7bec
  uid: 0
  URI: /livetest/huawei1.flv
  ```

  Obtain **md5hash** using the calculation formula.

  ```
  HashValue = md5sum("/livetest/huawei1.flv-1592639100-477b3bbc253f467b8def6711128c7bec-0-
  GCTbw44s6MPLh4GqgDpnfuFHgy25Enly") = dd1b5ffa00cf26acec0c169ae1cfabea
  ```

  The signed streaming URL is:

  ```
  http://test-play.example.com/livetest/huawei1.flv?
  auth_key=1592639100-477b3bbc253f467b8def6711128c7bec-0-dd1b5ffa00cf26acec0c169ae1cfabea
  ```

- **LLL**

  Generating a signed streaming URL is used as an example.

  ```
  Original URL: webrtc//test-play.example.com/livetest/huawei1
  timestamp: 1592639100
  Validity period: 1800s
  Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
  rand: 477b3bbc253f467b8def6711128c7bec
  uid: 0
  URI: /livetest/huawei1.sdp
  ```

  Obtain **md5hash** using the calculation formula.

  ```
  HashValue = md5sum("/livetest/huawei1.sdp-1592639100-477b3bbc253f467b8def6711128c7bec-0-
  GCTbw44s6MPLh4GqgDpnfuFHgy25Enly") = dd1b5ffa00cf26acec0c169ae1cfabea
  ```

  The signed streaming URL is:

  ```
  webrtc://test-play.example.com/livetest/huawei1?
  auth_key=1592639100-477b3bbc253f467b8def6711128c7bec-0-dd1b5ffa00cf26acec0c169ae1cfabea
  ```

Signing Method B

A signed string is calculated based on the **Key**, **timestamp**, and **Stream Name**.

Signed URL format:

```
Original URL?txSecret=md5(Key + Stream Name + txTime)&txTime=hex(timestamp)
```

Table 11-8 Authentication fields

Field	Description
txTime	Effective time of a streaming URL. The value is a hexadecimal Unix timestamp. If the value of **txTime** is greater than the requested time, the playback is normal. Otherwise, the playback is rejected. Example: 5eed5888 (that is, 2020.06.20 08:30:00)
Key	Key value set on the console. For details, see **URL Validation**
txSecret	Encryption parameter in the URL. The value is obtained by using the MD5 encryption algorithm to encrypt the string consisting of **key**, **Stream Name**, and **txTime**. `txSecret = md5 (Key + Stream Name + txTime)`
Duration	How long a signed URL remains effective. If **txTime** is set to the current time and the validity period is set to 1249s, the streaming URL expiration time is the current time plus 1249s.

Signed URL example:

- **Cloud Stream Live**

  Generating a signed streaming URL is used as an example.

  ```
  Original URL: http://test-play.example.com/livetest/huawei1.flv
  Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
  Stream Name: huawei1
  txTime: 5eed5888
  Duration: 1249s
  ```

  Obtain **txSecret** based on the calculation formula.

  ```
  txSecret = md5(GCTbw44s6MPLh4GqgDpnfuFHgy25Enlyhuawei15eed5888) =
  5cdc845362c332a4ec3e09ac5d5571d6
  ```

  The signed streaming URL is:

  ```
  http://test-play.example.com/livetest/huawei1.flv?
  txSecret=5cdc845362c332a4ec3e09ac5d5571d6&txTime=5eed5888
  ```

- **LLL**

  Generating a signed streaming URL is used as an example.

  ```
  Original URL: webrtc://test-play.example.com/livetest/huawei1
  Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
  Stream Name: huawei1
  txTime: 5eed5888
  Duration: 1249s
  ```

  Obtain **txSecret** based on the calculation formula.

  ```
  txSecret = md5(GCTbw44s6MPLh4GqgDpnfuFHgy25Enlyhuawei15eed5888) =
  5cdc845362c332a4ec3e09ac5d5571d6
  ```

  The signed streaming URL is:

  ```
  webrtc://test-play.example.com/livetest/huawei1?
  txSecret=5cdc845362c332a4ec3e09ac5d5571d6&txTime=5eed5888
  ```

Signing Method C

A signed string is calculated based on the **Key**, **Timestamp**, **App Name**, **Stream Name**, and **CheckLevel**.

Signed URL format:

```
Original URL?auth_info={Encrypted string}.{EncodedIV}
```

The algorithm for generating the authentication fields is as follows. For details about the code example, see **Code Example**.

- LiveID = <App Name>+"/"+<Stream Name>
- Encrypted string = UrlEncode(Base64(AES128(<Key>,"$"+<Timestamp>+"$"+<LiveID>+"$"+<CheckLevel>)))
- EncodedIV = Hex (IV used for encryption)

Table 11-9 describes encryption parameters in the algorithm.

Table 11-9 Encryption parameters

Field	Description
App Name	Application name, which is the same as the value of **App Name** in an ingest or streaming URL
Stream Name	Stream name, which is the same as the value of **Stream Name** in an ingest or streaming URL
Key	Key value set on the console. For details, see **URL Validation**
LiveID	Livestream ID, which uniquely identifies a livestream. The value consists of **App Name** and **Stream Name**. `LiveID = <App Name>+"/"+<Stream Name>`
Timestamp	UTC time when an authentication parameter is generated, in **yyyyMMddHHmmss** format. This parameter is used to check whether the authentication parameter has expired, that is, whether the absolute value of the difference between **Timestamp** and the current time is greater than the configured timeout interval.
CheckLevel	Check level. The value is **3** or **5**. ● If **CheckLevel** is **3**, the system only checks whether the value of **LiveID** is matched. ● If **CheckLevel** is **5**, the system checks whether the value of **LiveID** is matched and whether **Timestamp** times out.
IV	Cipher block chaining (CBC) depends on the initialization vector (IV). IV consists of 16 random digits and letters and must be 128 bits. In CBC mode, PKCS7 padding is used.

Signed URL example:

- **Cloud Stream Live**

  Generating a signed streaming URL is used as an example.

  ```
  Original URL: http://test-play.example.com/livetest/huawei1.flv
  App Name: livetest
  Stream Name: huawei1
  Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
  LiveID: livetest/huawei1
  Timestamp: 20190428110000
  CheckLevel: 3
  IV: yCmE666N3YAq30SN
  ```

  The encrypted string and EncodedIV are obtained according to the calculation formula.

  ```
  Encrypted string = I90KW7GhxOMwoy5yaeKMStZsOC %2B6WIyqU2kLBYAvcso %3D
  EncodIV = 79436d453636364e335941713330534e
  ```

  The signed streaming URL is:

  ```
  http://test-play.example.com/livetest/huawei1.flv?auth_info=I90KW7GhxOMwoy5yaeKMStZsOC
  %2B6WIyqU2kLBYAvcso%3D.79436d453636364e335941713330534e
  ```

- **LLL**

  Generating a signed streaming URL is used as an example.

  ```
  Original URL: webrtc://test-play.example.com/livetest/huawei1
  App Name: livetest
  Stream Name: huawei1
  Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
  LiveID: livetest/huawei1
  Timestamp: 20190428110000
  CheckLevel: 3
  IV: yCmE666N3YAq30SN
  ```

  The encrypted string and EncodedIV are obtained according to the calculation formula.

  ```
  Encrypted string = I90KW7GhxOMwoy5yaeKMStZsOC %2B6WIyqU2kLBYAvcso %3D
  EncodIV = 79436d453636364e335941713330534e
  ```

  The signed streaming URL is:

  ```
  webrtc://test-play.example.com/livetest/huawei1?auth_info=I90KW7GhxOMwoy5yaeKMStZsOC
  %2B6WIyqU2kLBYAvcso%3D.79436d453636364e335941713330534e
  ```

Signing Method D

A signed string is calculated based on the **Key**, **timestamp**, and **Stream Name**.

Signed URL format:

```
Original URL?hwSecret=hmac_sha256(Key, Stream Name + hwTime)&hwTime=hex(timestamp)
```

Table 11-10 Authentication fields

Field	Description
hwTime	Effective time of a streaming URL. The value is a hexadecimal Unix timestamp. If the value of **hwTime + *duration*** is greater than the requested time, the playback is normal. Otherwise, the playback is rejected. Example: 5eed5888 (that is, 2020.06.20 08:30:00)
Key	Key value set on the console. For details, see **URL Validation**

Field	Description
hwSecret	Encryption parameter in the URL. The value is obtained using the HMAC-SHA256 algorithm, with *Key* and *Stream Name* + *hwTime* as parameters. `hwSecret = hmac_sha256 (Key, Stream Name + hwTime)`
Duration	How long a signed URL remains effective. If **hwTime** is set to the current time and the validity period is set to 1249s, the streaming URL expiration time is the current time plus 1249s.

Signed URL example:

- **Cloud Stream Live**

  Generating a signed streaming URL is used as an example.

  ```
  Original URL: http://test-play.example.com/livetest/huawei1.flv
  Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
  Stream Name: huawei1
  hwTime: 5eed5888
  Duration: 1249s
  ```

  Obtain **hwSecret** based on the calculation formula.

  ```
  hwSecret = hmac_sha256(GCTbw44s6MPLh4GqgDpnfuFHgy25Enly, huawei15eed5888) =
  ce201856a0957413319e883c8ccae13602f01d3d91e21daf5161964cf708a6a8
  ```

  The signed streaming URL is:

  ```
  http://test-play.example.com/livetest/huawei1.flv?
  hwSecret=ce201856a0957413319e883c8ccae13602f01d3d91e21daf5161964cf708a6a8&hwTime=5eed5
  888
  ```

- **LLL**

  Generating a signed streaming URL is used as an example.

  ```
  Original URL: webrtc://test-play.example.com/livetest/huawei1
  Key: GCTbw44s6MPLh4GqgDpnfuFHgy25Enly
  Stream Name: huawei1
  hwTime: 5eed5888
  Duration: 1249s
  ```

  Obtain **hwSecret** based on the calculation formula.

  ```
  hwSecret = hmac_sha256(GCTbw44s6MPLh4GqgDpnfuFHgy25Enly, huawei15eed5888) =
  ce201856a0957413319e883c8ccae13602f01d3d91e21daf5161964cf708a6a8
  ```

  The signed streaming URL is:

  ```
  webrtc://test-play.example.com/livetest/huawei1?
  hwSecret=ce201856a0957413319e883c8ccae13602f01d3d91e21daf5161964cf708a6a8&hwTime=5eed5
  888
  ```

Sample Code

The following is the code example for generating a signed string in method C:

```
import javax.crypto.Cipher;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;

import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;
```

```
public class Main {

        public static void main(String[] args) {

        // data="$"+<Timestamp>+"$"+<LiveID>+"$"+<CheckLevel>. For details, see "Signing Method C."
                String data = "$20190428110000$live/stream01$3";

                // A random 16-digit string consisting of digits and letters
        byte[] ivBytes = "yCmE666N3YAq30SN".getBytes();

                // Key value configured on the Live console
        byte[] key = "GCTbw44s6MPLh4GqgDpnfuFHgy25Enly".getBytes();

                String msg = aesCbcEncrypt(data, ivBytes, key);
        try {
            System.out.println(URLEncoder.encode(msg, "UTF-8") + "." + bytesToHexString(ivBytes));
        } catch (UnsupportedEncodingException e) {
            e.printStackTrace();
        }
    }

        private static String aesCbcEncrypt(String data, byte[] ivBytes, byte[] key) {
        try {
            SecretKeySpec sk = new SecretKeySpec(key, "AES");
            Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");

                        if (ivBytes != null) {
                cipher.init(Cipher.ENCRYPT_MODE, sk, new IvParameterSpec(ivBytes));
            } else {
                cipher.init(Cipher.ENCRYPT_MODE, sk);
            }

                        return Base64.encode(cipher.doFinal(data.getBytes("UTF-8")));
        } catch (Exception e) {
            return null;
        }
    }

        public static String bytesToHexString(byte[] src) {
        StringBuilder stringBuilder = new StringBuilder("");
        if ((src == null) || (src.length <= 0)) {
            return null;
        }

                for (int i = 0; i < src.length; i++) {
            int v = src[i] & 0xFF;
            String hv = Integer.toHexString(v);
            if (hv.length() < 2) {
                stringBuilder.append(0);
            }
            stringBuilder.append(hv);
        }
        return stringBuilder.toString();
    }
}
```

Base64 is used to encode encrypted strings.

```
public class Base64
{

    / ** Base64 encoding table */
    private static char base64Code[] =
    {
        'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R',
        'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z', 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j',
        'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', '0', '1',
        '2', '3', '4', '5', '6', '7', '8', '9', '+', '/',};

    /**
```

```
     * The construction method is privatized to prevent instantiation.
     */
    private Base64()
    {
        super();
    }

    /**
     * Encode three bytes in a byte array into four visible characters.
     * @param bytes Byte data to be encoded
     * @return Base64 character string after encoding
     */
    public static String encode(byte[] bytes)
    {
        int a = 0;

        // Allocate memory based on the actual length after encoding for acceleration.
        StringBuffer buffer = new StringBuffer(((bytes.length - 1) / 3) << 2 + 4);

        // Encoding
        for (int i = 0; i < bytes.length; i++)
        {
            a |= (bytes[i] << (16 - i % 3 * 8)) & (0xff << (16 - i % 3 * 8));
            if (i % 3 == 2 || i == bytes.length - 1)
            {
                buffer.append(Base64.base64Code[(a & 0xfc0000) >>> 18]);
                buffer.append(Base64.base64Code[(a & 0x3f000) >>> 12]);
                buffer.append(Base64.base64Code[(a & 0xfc0) >>> 6]);
                buffer.append(Base64.base64Code[a & 0x3f]);
                a = 0;
            }
        }

        // For a byte array whose length is not an integral multiple of 3, add 0 before encoding and replace it
with = after encoding.
        // The number of equal signs (=) is the same as the length of the missing data to identify the actual
data length.
        if (bytes.length % 3 > 0)
        {
            buffer.setCharAt(buffer.length() - 1, '=');
        }
        if (bytes.length % 3 == 1)
        {
            buffer.setCharAt(buffer.length() - 2, '=');
        }
        return buffer.toString();
    }

}
```

11.5.4 ACL

You can add the IP addresses that are allowed or not allowed to play content to the whitelist or blacklist. CDN allows or rejects the playback requests based on the whitelist or blacklist.

Notes

- This function is optional and is disabled by default.
- Whitelists and blacklists cannot be used simultaneously.
- A maximum of 100 IP addresses can be added to a whitelist or blacklist.

Prerequisites

- The ingest domain name and streaming domain name have been **added** and **associated**.
- You have **configured CNAME records** at your domain names' DNS provider.

Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Domains**.

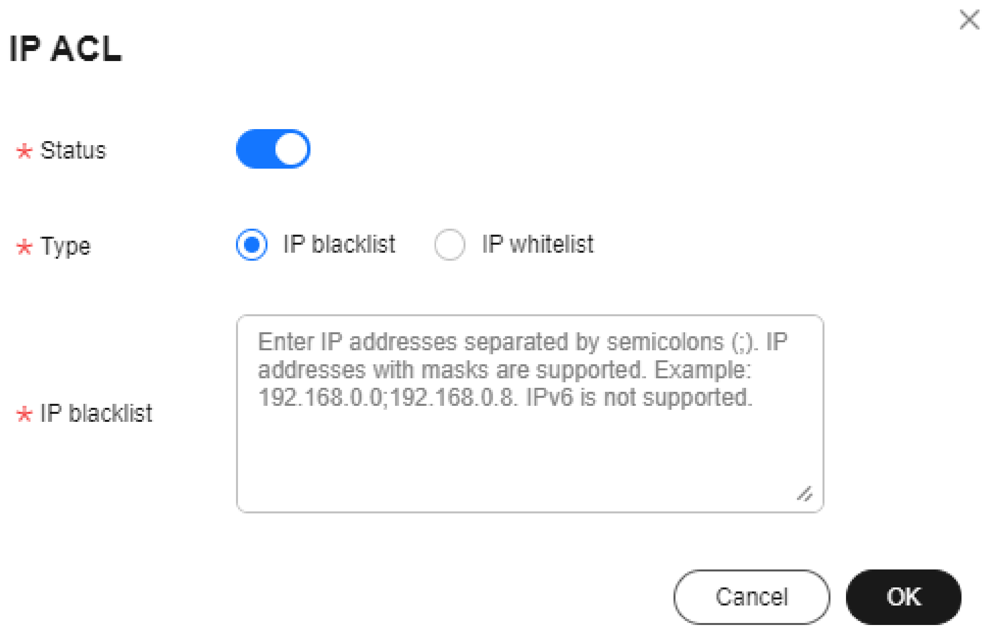
Step 3 Click **Manage** in the **Operation** column of the desired streaming domain name.

Step 4 In the navigation pane, choose **Basic Settings** > **Access Control**.

Step 5 Click **IP ACL**. The **IP ACL** dialog box is displayed.

Step 6 Toggle on the switch and configure an IP address blacklist or whitelist, as shown in **Figure 11-15**.

Figure 11-15 Configuring an ACL



IP ACL

* Status: on

* Type: ● IP blacklist ○ IP whitelist

* IP blacklist: Enter IP addresses separated by semicolons (;). IP addresses with masks are supported. Example: 192.168.0.0;192.168.0.8. IPv6 is not supported.

Step 7 Select **IP address blacklist** or **IP address whitelist**, and enter an IP address or IP address range. IPv6 is not supported.

Step 8 Click **OK**.

----End

12 Streaming

12.1 Streams

You can view the online streaming status in real time. You can disable a livestream, so its ingest URL cannot be used to push the stream. You can also resume the livestream to allow stream push using the ingest URL.

Viewing Stream Push Information

⚠ CAUTION

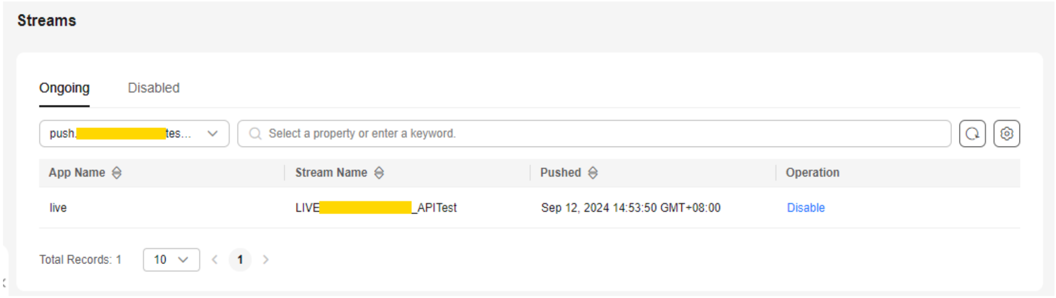
After a livestream is pushed successfully, it takes about 2 to 4 minutes to view its information.

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Streaming** > **Streams**.

Step 3 Select a domain name to view information about a livestream being pushed.

Figure 12-1 Viewing stream push information



App Name	Stream Name	Pushed	Operation
live	LIVE[redacted]_APITest	Sep 12, 2024 14:53:50 GMT+08:00	Disable

Total Records: 1 10 < 1 >

----End

Disabling Stream Push

Only a livestream that is being pushed can be disabled. After a livestream is disabled, the ingest URL cannot be used to push livestreams.

To disable a livestream, perform the following operations:

Step 1 Log in to the **Live console**.

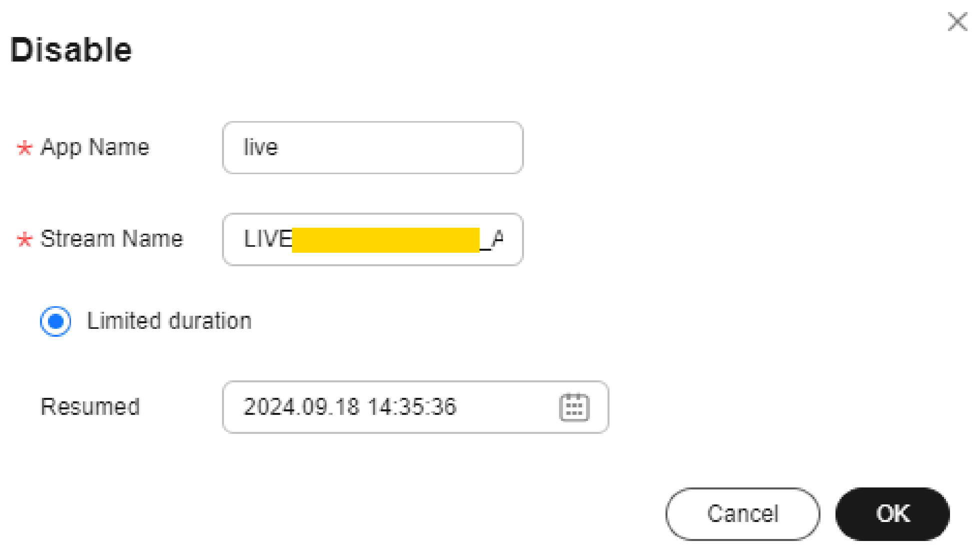
Step 2 In the navigation pane, choose **Streaming** > **Streams**.

Step 3 Locate the domain name for which stream push is to be disabled.

Step 4 Click **Disable** in the **Operation** column.

Select the time when stream push is resumed. You can view information about disabled livestreams on the **Disabled** tab.

Figure 12-2 Configuration of disabling stream push



Disable

* App Name: live

* Stream Name: LIVE[redacted]_A

● Limited duration

Resumed: 2024.09.18 14:35:36

Limited duration: The livestream cannot be pushed until the time indicated by **Resumed** arrives. Livestreams can be disabled for up to 90 days.

----End

Resuming Stream Push

To resume stream push for a domain name, perform the following operations:

Step 1 Log in to the **Live console**.

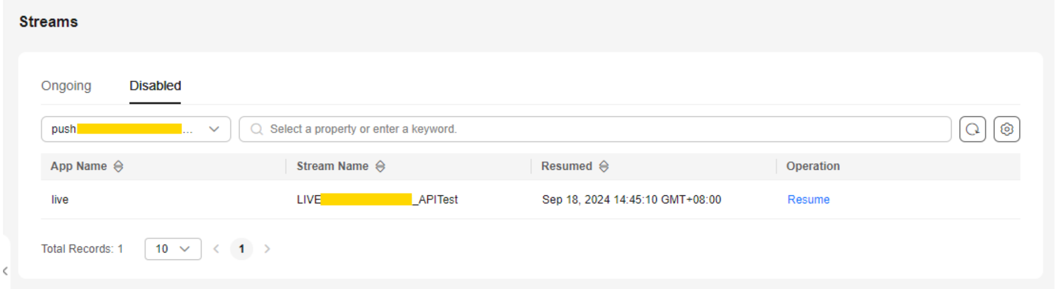
Step 2 In the navigation pane, choose **Streaming** > **Streams**.

Step 3 Select the domain name for which stream push needs to be resumed from the drop-down list.

Step 4 Click the **Disabled** tab.

Step 5 Click **Resume** in the **Operation** column.

Figure 12-3 Resuming stream push



Streams

App Name	Stream Name	Resumed	Operation
live	LIVE[redacted]_APITest	Sep 18, 2024 14:45:10 GMT+08:00	Resume

----End

13 Usage Statistics

You can check the downstream bandwidth/traffic of all streaming domain names, and the total transcoding duration, maximum number of concurrent recording streams, and number of snapshots of all ingest domain names.

About Query

- You can query bandwidth/traffic data of the past 24 hours.
- You can query transcoding/recording/snapshot data of the past 90 days. The maximum query time span is 31 days.

Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Usage Statistics**.

Step 3 View statistics on the **Bandwidth/Traffic**, **Transcoding**, **Recording**, or **Snapshot** tab.

----End

Bandwidth/Traffic

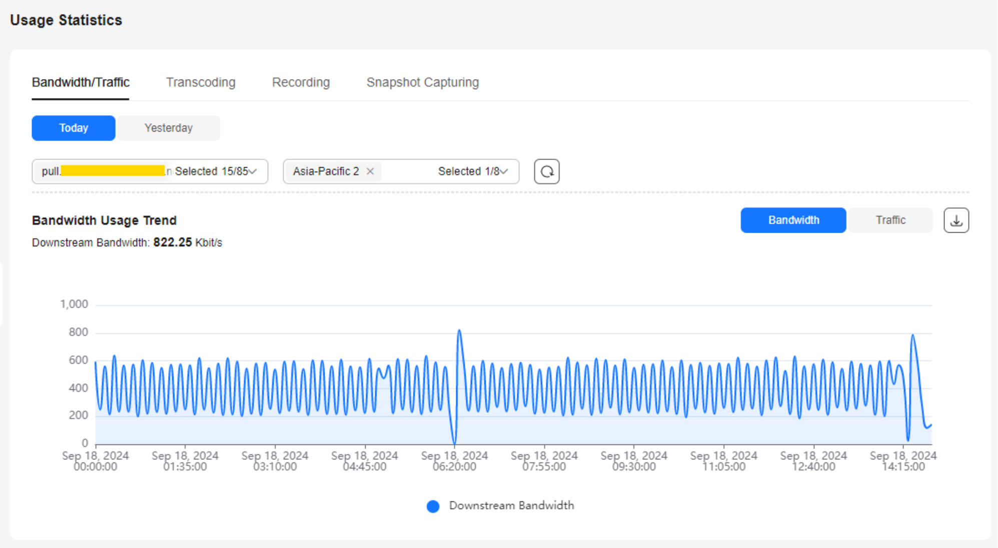
Specify the time, streaming domain name, and billing region to view data in the **Bandwidth Usage Trend** or **Traffic Usage Trend** area.

You can click ↗ to export the downstream bandwidth or traffic details.

- **Bandwidth Usage Trend** displays the bandwidth usage trend of a selected domain name.

  You can point to the chart to view the specific value or scroll the mouse wheel to zoom in or out on the X-axis within a time range.

Figure 13-1 Downstream bandwidth trend



Usage Statistics

Bandwidth/Traffic | Transcoding | Recording | Snapshot Capturing

Today | Yesterday

pull.[redacted]n Selected 15/85 | Asia-Pacific 2 × Selected 1/8

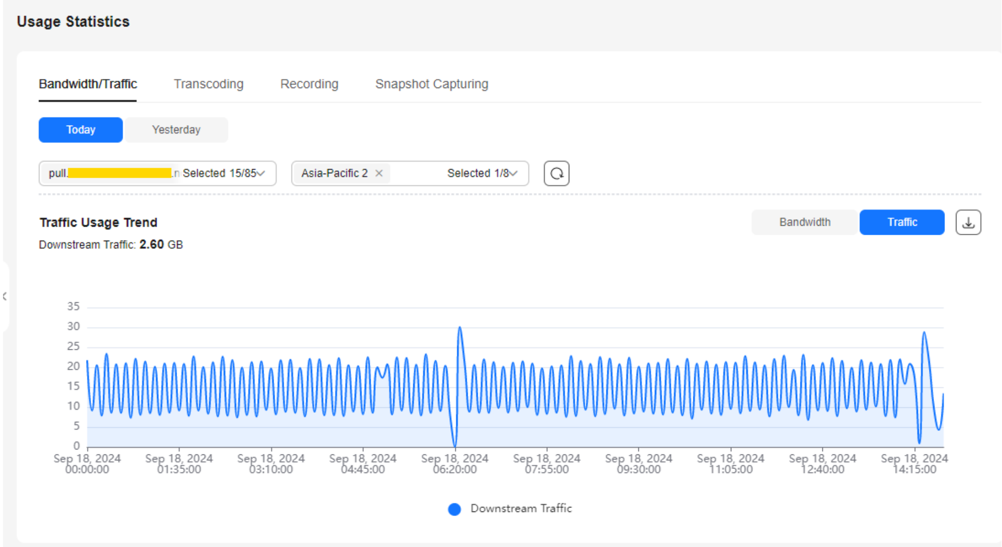
Bandwidth Usage Trend

Downstream Bandwidth: 822.25 Kbit/s

- **Traffic Usage Trend** displays the traffic usage trend of a selected domain name.

  You can point to the chart to view the specific value or scroll the mouse wheel to zoom in or out on the X-axis within a time range.

Figure 13-2 Downstream traffic details



Usage Statistics

Bandwidth/Traffic | Transcoding | Recording | Snapshot Capturing

Today | Yesterday

pull.[redacted]n Selected 15/85 | Asia-Pacific 2 × Selected 1/8

Traffic Usage Trend

Downstream Traffic: 2.60 GB

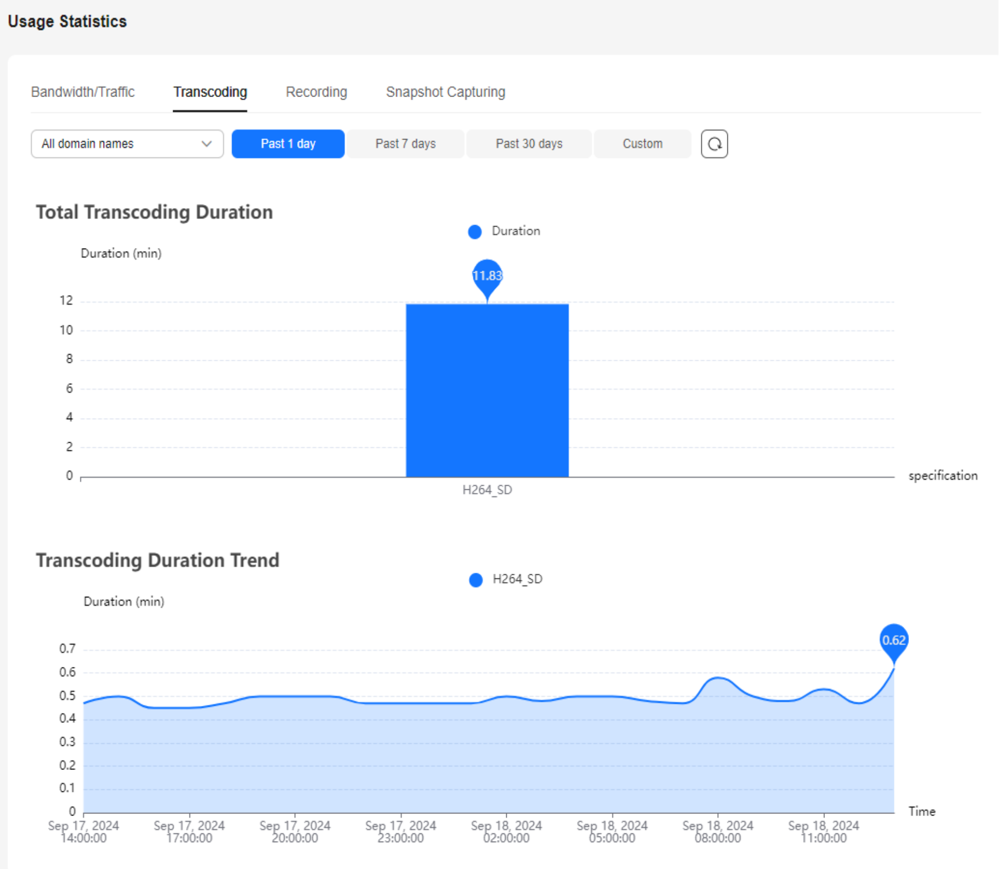
Transcoding

Specify the time and ingest domain name to view the total transcoding duration and transcoding duration trend.

- **Total Transcoding Duration** displays the total duration of different transcoded outputs of a selected domain name in the query period.
- **Transcoding Duration Trend** displays the total duration of different transcoded outputs of a selected domain name in the query period.

  You can point to the chart to view the specific value or scroll the mouse wheel to zoom in or out on the X-axis within a time range.

Figure 13-3 Transcoding



Recording

The system collects statistics on the total number of concurrent recording streams every 5 minutes and obtains 12 values every hour. It then uses the maximum value as the number of concurrent recording streams in the hour.

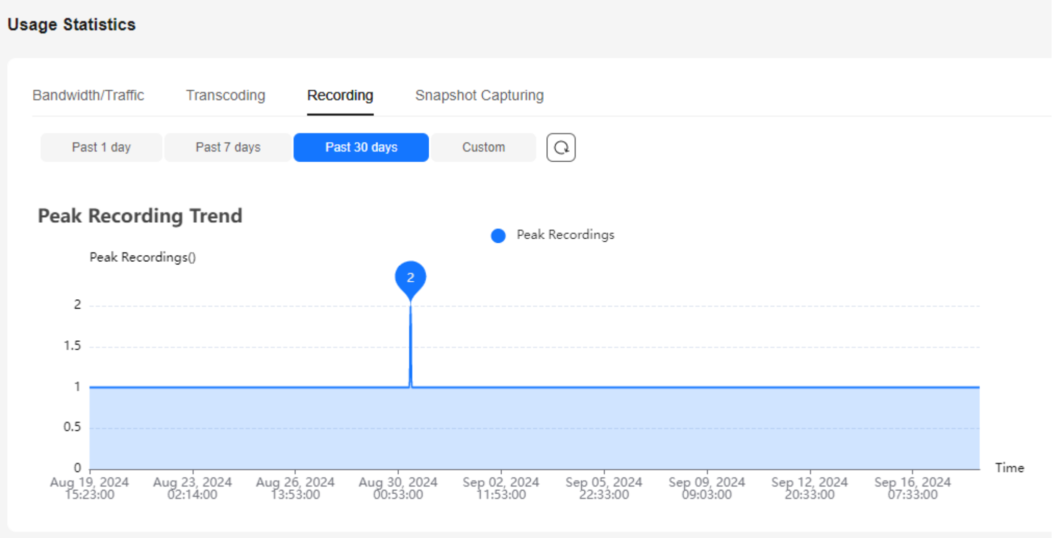
Specify the time to view the peak recording trend.

The peak recording trend area displays the maximum number of recorded concurrent livestreams of an account per hour, as shown in **Figure 13-4**.

You can point to the chart to view the specific value or scroll the mouse wheel to zoom in or out on the X-axis within a time range.

You can point to the chart to view the specific value or scroll the mouse wheel to zoom in or out on the X-axis within a time range.

Figure 13-4 Peak concurrent recording stream trends



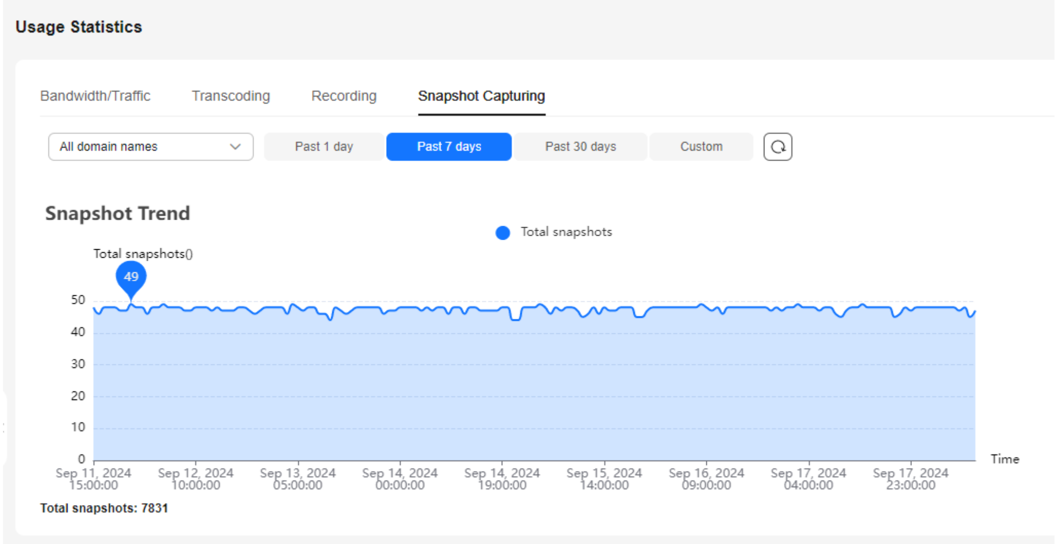
Snapshot

Specify the time and ingest domain name to view the number of snapshots.

The **Screenshot Trends** area displays the number of snapshots captured for a selected domain name during livestream push, as shown in **Figure 13-5**.

You can point to the chart to view the specific value or scroll the mouse wheel to zoom in or out on the X-axis within a time range.

Figure 13-5 Snapshot trends



Total snapshots: 7831

14 Service Monitoring

You can view the downstream bandwidth/traffic, playback profiles, status codes returned in the request response of a streaming domain name, and the number of online viewers of the corresponding livestream. You can also view monitoring information such as the upstream bandwidth/traffic, total number of pushed streams, streaming records, and stream push frame rate/bitrate of an ingest domain name.

Notes

The number system of bandwidth is 1,024. For example, 1 Mbit/s is equal to 1024 Kbit/s.

Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Service Monitoring**.

Step 3 Select **Downstream Bandwidth/Traffic**, **Upstream Bandwidth/Traffic**, **Status Codes**, **Streams**, **Pushed Streams**, **Streaming Records**, **Stream Playback Profiles**, or **Stream Push Monitoring** to view statistics.

Move the cursor to the trend chart and scroll the mouse wheel to zoom in or zoom out the X axis (time).

----End

Downstream Bandwidth/Traffic

Specify the time, streaming domain name, area, app name, stream name, statistical granularity, and packaging protocol. Click **Bandwidth** or **Traffic** on the right of the page to view the bandwidth or traffic usage trend.

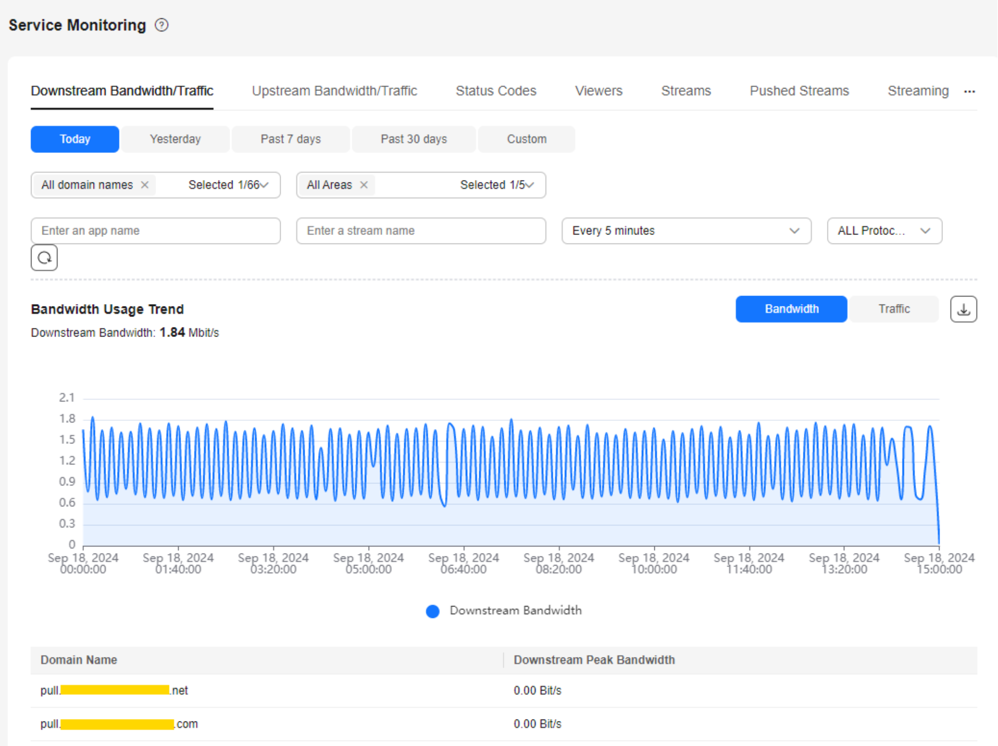
You can click ⤓ on the right to export specific data.

NOTE

- You can query statistics of the past 365 days.
- You can query statistics in a time span of up to 31 days.
- The minimum statistical granularity is five minutes. For example, data generated from November 6, 2020 08:00:00 (GMT+08:00) to November 6, 2020 08:04:59 (GMT+08:00) is displayed at the statistical point November 6, 2020 08:00:00 (GMT+08:00). The bandwidth uses the average value of the selected statistical granularity, and the traffic uses the accumulated value of the selected statistical granularity.
- The stream name is the name of the stream pulled by the player. For example, if the player pulls a transcoded stream, set the stream name to the name of the transcoded stream.
- The exported data cannot be classified by carrier.

- **Bandwidth Usage Trend** displays the bandwidth usage trend of the selected domain name. You can also view the downstream peak bandwidth of the selected domain name within the query period below the **Bandwidth Usage Trend** area, as shown in **Figure 14-1**.

Figure 14-1 Downstream bandwidth statistics



Service Monitoring

Downstream Bandwidth/Traffic | Upstream Bandwidth/Traffic | Status Codes | Viewers | Streams | Pushed Streams | Streaming ···

Today | Yesterday | Past 7 days | Past 30 days | Custom

All domain names × Selected 1/66 | All Areas × Selected 1/5

Enter an app name | Enter a stream name | Every 5 minutes | ALL Protoc...

Bandwidth Usage Trend

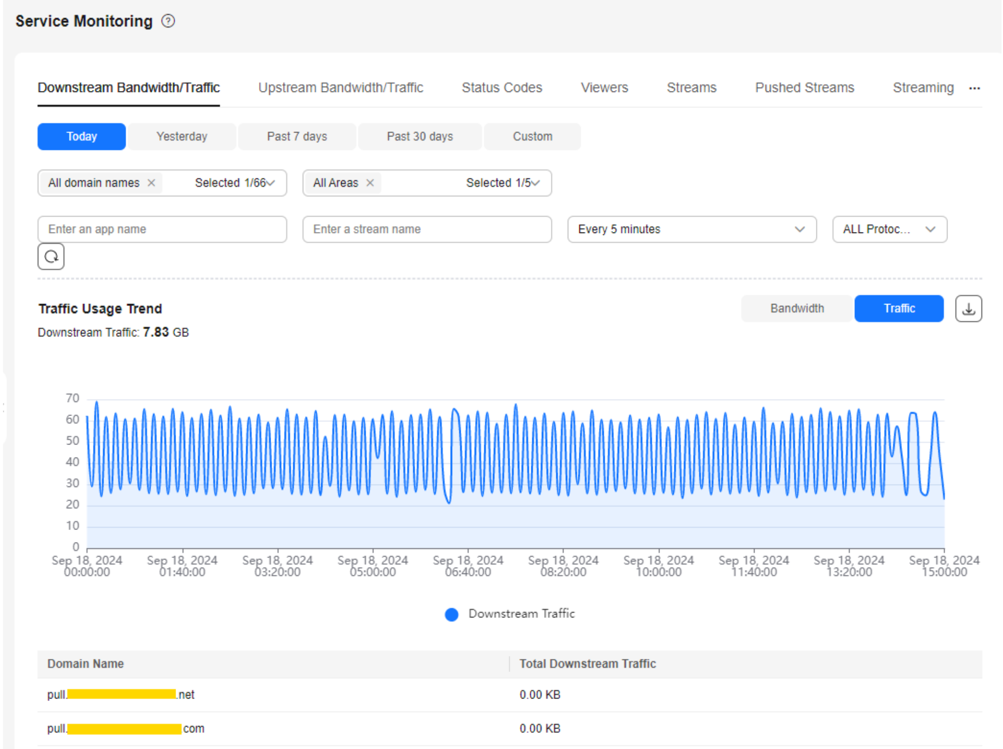
Downstream Bandwidth: **1.84** Mbit/s

Bandwidth | Traffic

Domain Name	Downstream Peak Bandwidth
pull.[redacted].net	0.00 Bit/s
pull.[redacted].com	0.00 Bit/s

- **Traffic Usage Trend** displays the traffic usage trend of the selected domain name. You can also view the traffic consumption of the selected domain name within the query period below the **Traffic Usage Trend** area, as shown in **Figure 14-2**.

Figure 14-2 Downstream traffic statistics



Downstream Traffic: 7.83 GB

Domain Name	Total Downstream Traffic
pull.[redacted].net	0.00 KB
pull.[redacted].com	0.00 KB

NOTICE

The total traffic displayed in the traffic table and traffic trend chart is the sum of traffic measured every five minutes and converted from byte into MB, accurate to two decimal places. Therefore, the displayed traffic data may be slightly different from the sum of the values in the **Downstream Traffic(MB)** column in the exported traffic statistics table. This is because the values are rounded off.

Upstream Bandwidth/Traffic

Specify the time, ingest domain name, area, province/state, carrier, app name, stream name, statistical granularity, and packaging protocol. Click **Bandwidth** or **Traffic** on the right of the page to view the bandwidth or traffic usage trend.

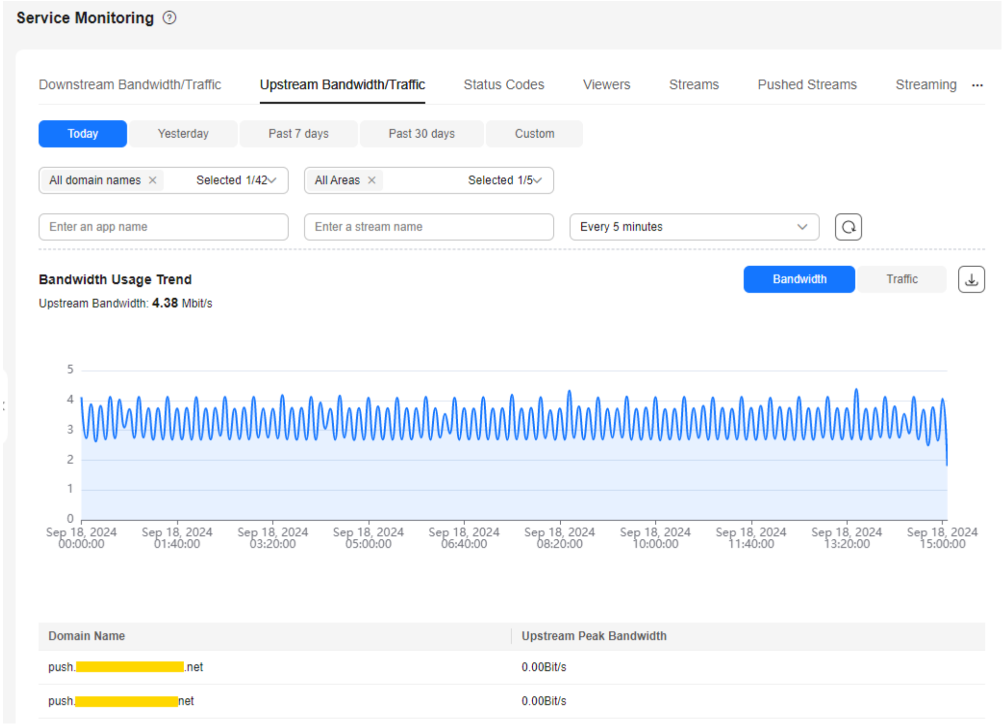
You can click ⤓ on the right to export specific data.

NOTE

- You can query statistics of the past 365 days.
- You can query statistics in a time span of up to 31 days.
- The minimum statistical granularity is five minutes. For example, data generated from November 6, 2020 08:00:00 (GMT+08:00) to November 6, 2020 08:04:59 (GMT+08:00) is displayed at the statistical point November 6, 2020 08:00:00 (GMT+08:00). The bandwidth uses the average value of the selected statistical granularity, and the traffic uses the accumulated value of the selected statistical granularity.
- The exported data cannot be classified by carrier.

- **Bandwidth Usage Trend** displays the upstream bandwidth usage trend of the selected domain name, as shown in **Figure 14-3**.

Figure 14-3 Upstream bandwidth trend



All domain names × Selected 1/42

All Areas × Selected 1/5

Enter an app name

Enter a stream name

Every 5 minutes

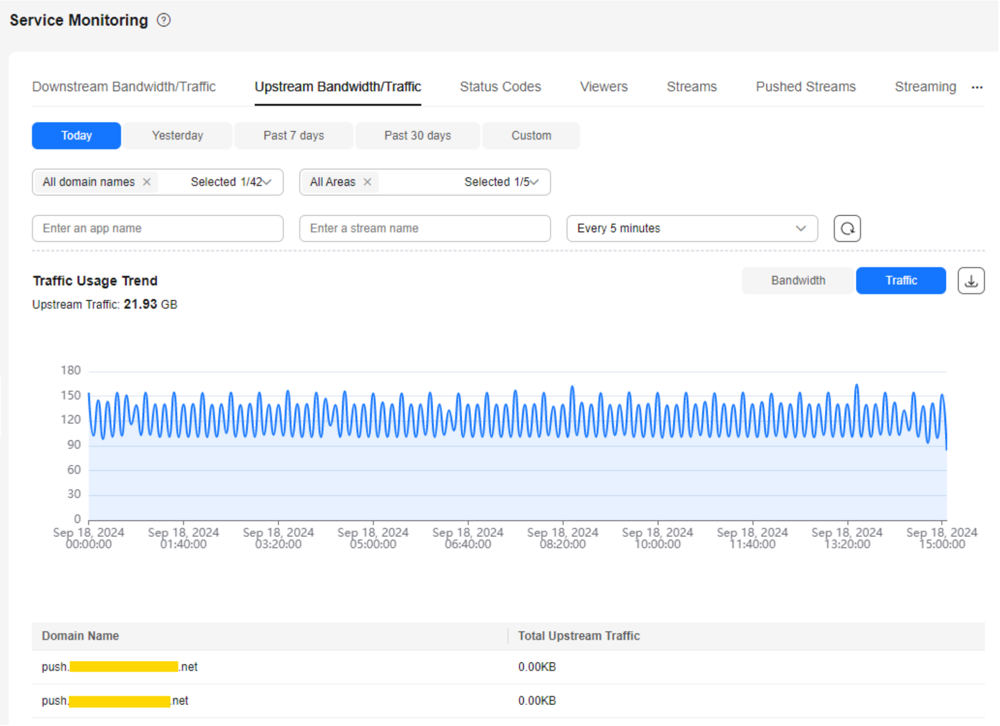
Bandwidth Usage Trend

Upstream Bandwidth: **4.38** Mbit/s

Domain Name	Upstream Peak Bandwidth
push.[redacted].net	0.00Bit/s
push.[redacted]net	0.00Bit/s

- **Traffic Usage Trend** displays the traffic usage trend of the selected domain name. You can also view the traffic consumption of the selected domain name within the query period below the **Traffic Usage Trend** area, as shown in **Figure 14-4**.

Figure 14-4 Upstream traffic statistics



All domain names × Selected 1/42

All Areas × Selected 1/5

Enter an app name

Enter a stream name

Every 5 minutes

Traffic Usage Trend

Upstream Traffic: **21.93** GB

Domain Name	Total Upstream Traffic
push.[redacted].net	0.00KB
push.[redacted].net	0.00KB

NOTICE

The total traffic displayed in the traffic table and traffic trend chart is the sum of traffic measured every five minutes and converted from byte into MB, accurate to two decimal places. Therefore, the displayed traffic data may be slightly different from the sum of the values in the **Downstream Traffic(MB)** column in the exported traffic statistics table. This is because the values are rounded off.

Status Codes

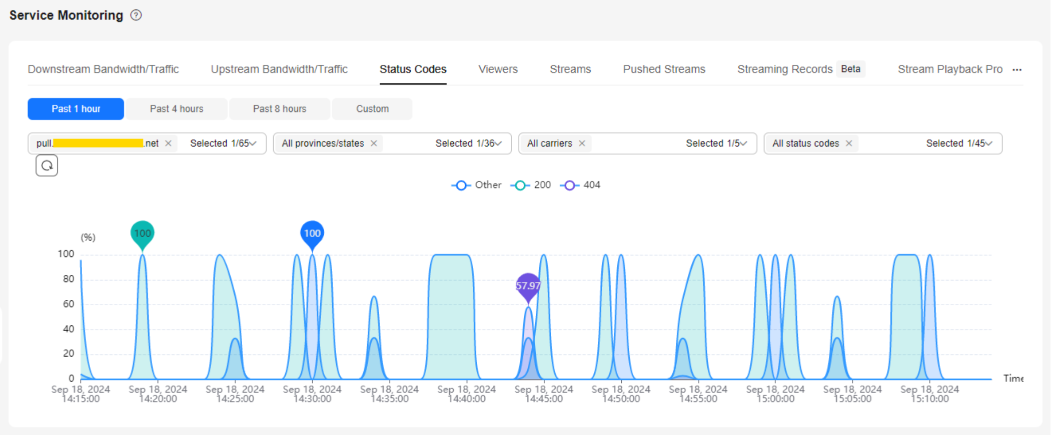
Specify the time, domain name, province/state, carrier, and status code, as shown in **Figure 14-5**.

NOTE

- You can query statistics of the past seven days.
- You can query statistics in a time span of up to one day.
- You can query statistics about up to 10 domain names at a time.
- The minimum statistical granularity is one minute. For example, data generated from November 6, 2020 08:00:00 (GMT+08:00) to November 6, 2020 08:00:59 (GMT+08:00) is displayed at the statistical point November 6, 2020 08:00:00 (GMT+08:00).

The trend chart displays the status codes returned by the selected domain name in the query period.

Figure 14-5 Status code statistics



Streams

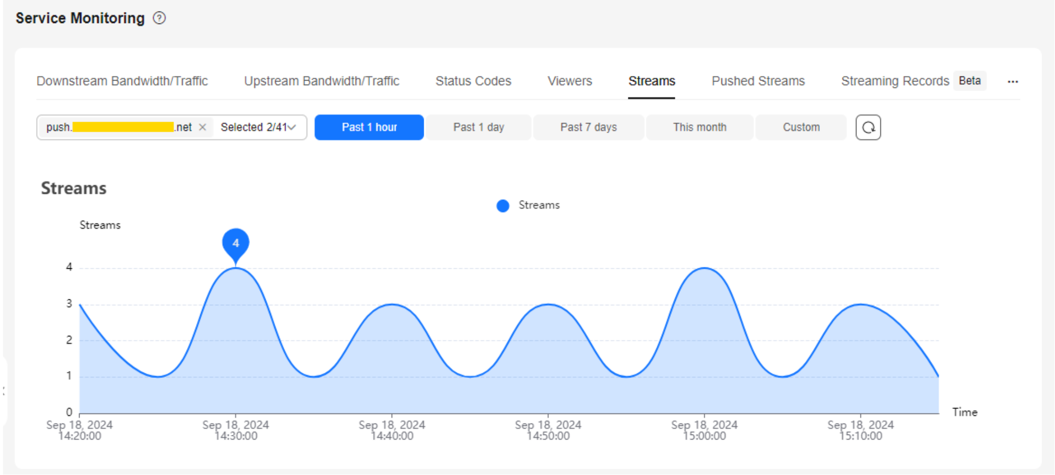
Specify the ingest domain name and time.

NOTE

- You can query statistics of the past 365 days.
- You can query statistics in a time span of up to 31 days.
- You can query statistics about up to 10 domain names at a time.
- The minimum statistical granularity is five minutes. For example, data generated from November 6, 2020 08:00:00 (GMT+08:00) to November 6, 2020 08:04:59 (GMT+08:00) is displayed at the statistical point November 6, 2020 08:00:00 (GMT+08:00). The displayed data is the maximum value of the selected statistical granularity.

The trend chart displays the trend of the total number of streams (of the selected domain name) pushed to the Live origin server, as shown in **Figure 14-6**.

Figure 14-6 Streams



Pushed Streams

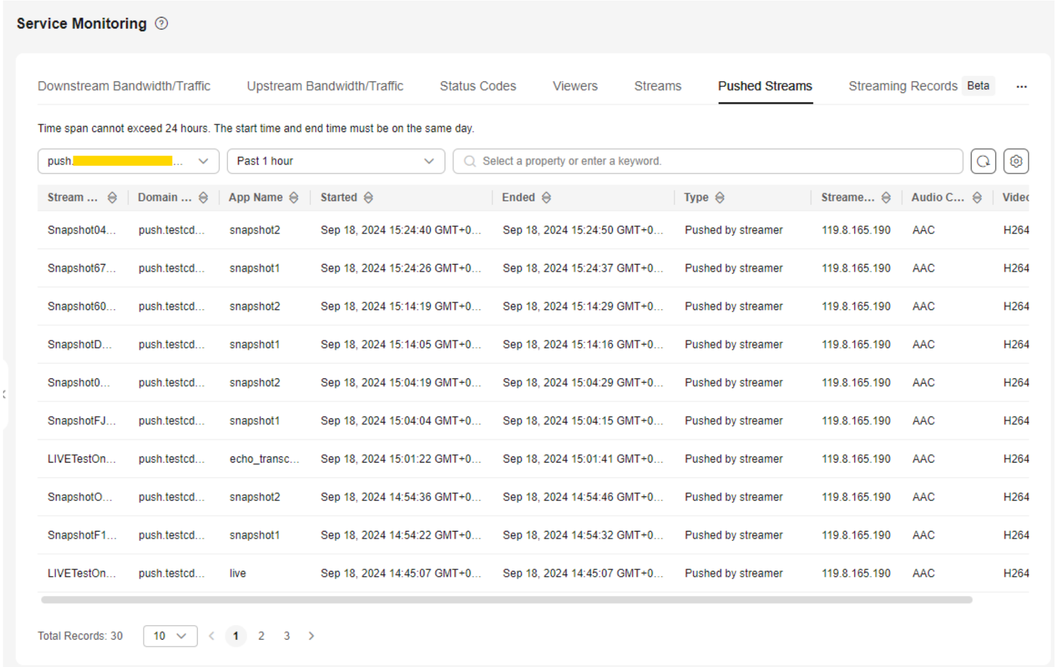
Specify the time, ingest domain name, app name, and stream name. Click ↻ to view details about the pushed streams of the ingest domain name, as shown in **Figure 14-7**.

See **Table 14-1**.

NOTE

- The pushed streams of a domain name that is pushing streams cannot be queried.
- You can query statistics of the past seven days.
- You can query statistics in a time span of up to one day.

Figure 14-7 Pushed stream details



Time span cannot exceed 24 hours. The start time and end time must be on the same day.

push.[redacted]... | Past 1 hour | Select a property or enter a keyword.

Stream ...	Domain ...	App Name	Started	Ended	Type	Streame...	Audio C...	Videc
Snapshot04...	push.testcd...	snapshot2	Sep 18, 2024 15:24:40 GMT+0...	Sep 18, 2024 15:24:50 GMT+0...	Pushed by streamer	119.8.165.190	AAC	H264
Snapshot67...	push.testcd...	snapshot1	Sep 18, 2024 15:24:26 GMT+0...	Sep 18, 2024 15:24:37 GMT+0...	Pushed by streamer	119.8.165.190	AAC	H264
Snapshot60...	push.testcd...	snapshot2	Sep 18, 2024 15:14:19 GMT+0...	Sep 18, 2024 15:14:29 GMT+0...	Pushed by streamer	119.8.165.190	AAC	H264
SnapshotD...	push.testcd...	snapshot1	Sep 18, 2024 15:14:05 GMT+0...	Sep 18, 2024 15:14:16 GMT+0...	Pushed by streamer	119.8.165.190	AAC	H264
Snapshot0...	push.testcd...	snapshot2	Sep 18, 2024 15:04:19 GMT+0...	Sep 18, 2024 15:04:29 GMT+0...	Pushed by streamer	119.8.165.190	AAC	H264
SnapshotFJ...	push.testcd...	snapshot1	Sep 18, 2024 15:04:04 GMT+0...	Sep 18, 2024 15:04:15 GMT+0...	Pushed by streamer	119.8.165.190	AAC	H264
LIVETestOn...	push.testcd...	echo_transc...	Sep 18, 2024 15:01:22 GMT+0...	Sep 18, 2024 15:01:41 GMT+0...	Pushed by streamer	119.8.165.190	AAC	H264
SnapshotO...	push.testcd...	snapshot2	Sep 18, 2024 14:54:36 GMT+0...	Sep 18, 2024 14:54:46 GMT+0...	Pushed by streamer	119.8.165.190	AAC	H264
SnapshotF1...	push.testcd...	snapshot1	Sep 18, 2024 14:54:22 GMT+0...	Sep 18, 2024 14:54:32 GMT+0...	Pushed by streamer	119.8.165.190	AAC	H264
LIVETestOn...	push.testcd...	live	Sep 18, 2024 14:45:07 GMT+0...	Sep 18, 2024 14:45:07 GMT+0...	Pushed by streamer	119.8.165.190	AAC	H264

Total Records: 30 | 10 | < 1 2 3 >

Table 14-1 Parameters

Parameter	Description
Stream Name	Livestream name, that is, the custom value of **Stream Name** in the ingest URL.
Domain Name	Ingest domain name.
App Name	Application name, that is, the default or custom value of **App Name** in the ingest URL.
Started	Time when livestream push starts. The format is YYYY-MM-DD hh:mm:ss, for example, 2020-11-06 14:39:42.
Ended	Time when livestream push ends. The format is YYYY-MM-DD hh:mm:ss, for example, 2020-11-06 14:39:44.

Parameter	Description
Type	Stream push type, which can be **Pushed by streamer** or **Pulled from third-party CDN**.
Streamer IP	IP address of the stream push device.
Audio Coding	Audio codec.
Video Coding	Video codec.

Streaming Records

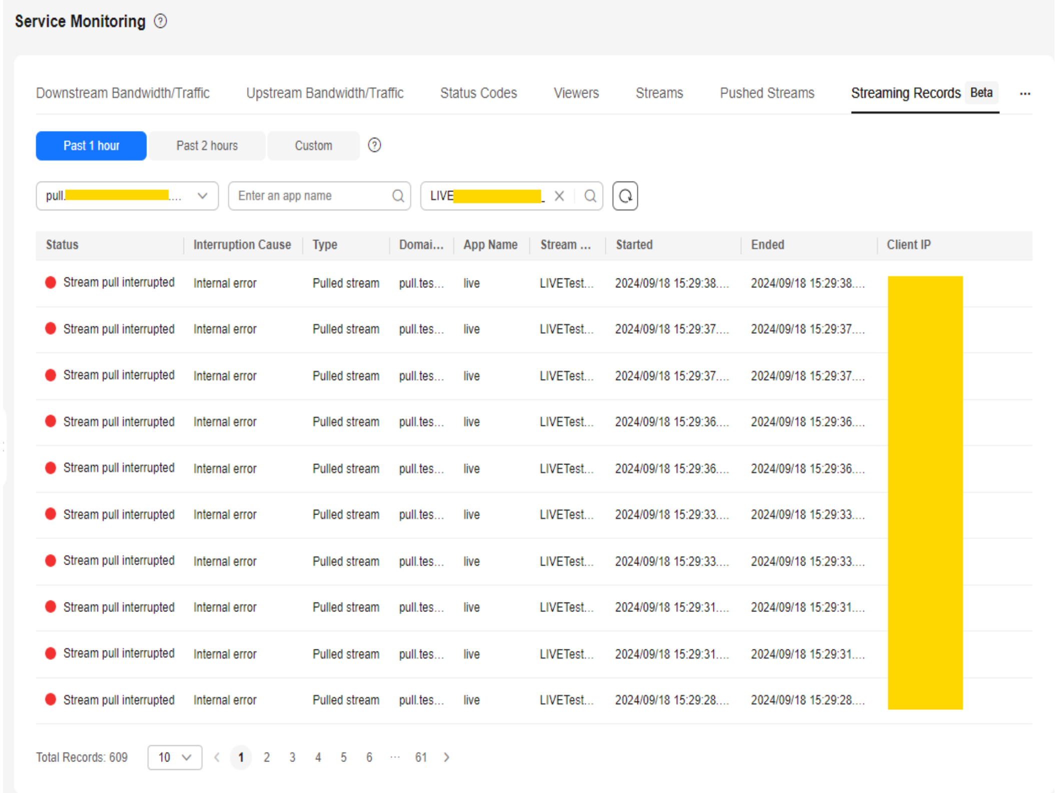
Specify the time, domain name, app name, and stream name. Click ↻ to view the streaming records of the selected domain name, as shown in **Figure 14-8**.

See **Table 14-2**.

NOTE

Due to a large amount of data, you can query statistics of the past 3 days and in a time span of up to 3 hours.

Figure 14-8 Streaming records



Service Monitoring

Downstream Bandwidth/Traffic | Upstream Bandwidth/Traffic | Status Codes | Viewers | Streams | Pushed Streams | Streaming Records Beta | ...

Past 1 hour | Past 2 hours | Custom

pull.[redacted].... | Enter an app name | LIVE[redacted]_

Status	Interruption Cause	Type	Domai...	App Name	Stream ...	Started	Ended	Client IP
● Stream pull interrupted	Internal error	Pulled stream	pull.tes...	live	LIVETest...	2024/09/18 15:29:38....	2024/09/18 15:29:38....	[redacted]
● Stream pull interrupted	Internal error	Pulled stream	pull.tes...	live	LIVETest...	2024/09/18 15:29:37....	2024/09/18 15:29:37....	[redacted]
● Stream pull interrupted	Internal error	Pulled stream	pull.tes...	live	LIVETest...	2024/09/18 15:29:37....	2024/09/18 15:29:37....	[redacted]
● Stream pull interrupted	Internal error	Pulled stream	pull.tes...	live	LIVETest...	2024/09/18 15:29:36....	2024/09/18 15:29:36....	[redacted]
● Stream pull interrupted	Internal error	Pulled stream	pull.tes...	live	LIVETest...	2024/09/18 15:29:36....	2024/09/18 15:29:36....	[redacted]
● Stream pull interrupted	Internal error	Pulled stream	pull.tes...	live	LIVETest...	2024/09/18 15:29:33....	2024/09/18 15:29:33....	[redacted]
● Stream pull interrupted	Internal error	Pulled stream	pull.tes...	live	LIVETest...	2024/09/18 15:29:33....	2024/09/18 15:29:33....	[redacted]
● Stream pull interrupted	Internal error	Pulled stream	pull.tes...	live	LIVETest...	2024/09/18 15:29:31....	2024/09/18 15:29:31....	[redacted]
● Stream pull interrupted	Internal error	Pulled stream	pull.tes...	live	LIVETest...	2024/09/18 15:29:31....	2024/09/18 15:29:31....	[redacted]
● Stream pull interrupted	Internal error	Pulled stream	pull.tes...	live	LIVETest...	2024/09/18 15:29:28....	2024/09/18 15:29:28....	[redacted]

Total Records: 609 | 10 | < 1 2 3 4 5 6 ··· 61 >

Table 14-2 Parameters

Parameter	Description
Status	Stream status. ● **Pushing streams/Pulling streams** ● **Stream push interrupted/Stream pull interrupted**
Interruption Cause	Cause for streaming interruption.
Type	Stream type. ● **Pulled stream** ● **Pushed stream**
Domain Name	Ingest or streaming domain name.
App Name	Application name, that is, the default or custom value of **App Name** in the ingest or streaming URL.
Stream Name	Stream name, that is, the custom value of **Stream Name** in the ingest or streaming URL.
Started	Time when the stream starts to be pushed or played. The format is YYYY/MM/DD HH:mm:ss.SSS [GMT]Z, for example, 2023-05-16 14:39:42.629 GMT+08:00.
Ended	Time when the stream stops being pushed or played. The format is YYYY/MM/DD HH:mm:ss.SSS [GMT]Z, for example, 2023-05-16 14:39:42.629 GMT+08:00.
Client IP	IP address of the stream push/pull device.

Stream Playback Profiles

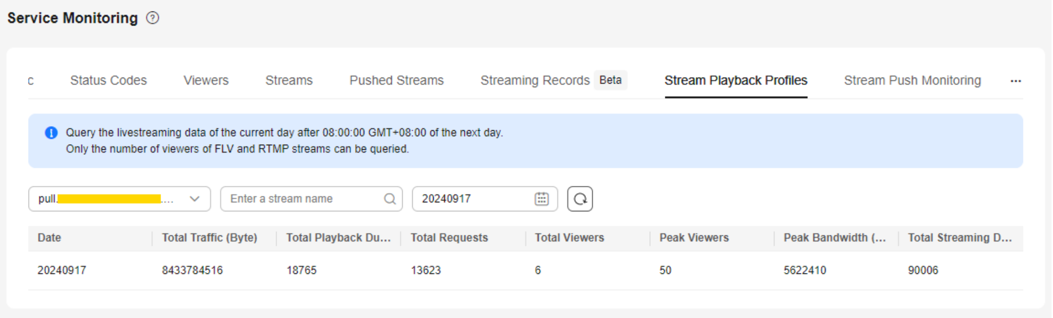
Specify the domain name, stream name, and time, as shown in **Figure 14-9**.

See **Table 14-3**.

NOTE

- You can query statistics of the past 31 days.
- You can query statistics in a time span of up to one day.
- Query the livestreaming data of the current day after 08:00:00 (GMT+08:00) of the next day.

Figure 14-9 Stream playback profiles



Query the livestreaming data of the current day after 08:00:00 GMT+08:00 of the next day.
Only the number of viewers of FLV and RTMP streams can be queried.

pull.[redacted]....

Enter a stream name

20240917

Date	Total Traffic (Byte)	Total Playback Du...	Total Requests	Total Viewers	Peak Viewers	Peak Bandwidth (...	Total Streaming D...
20240917	8433784516	18765	13623	6	50	5622410	90006

Table 14-3 Parameters

Parameter	Description
Date	Playback profile information from 00:00 to 23:59 on the selected date is collected. The format is YYYYMMDD, for example, 20201104.
Total Traffic (Byte)	Total traffic consumed during playback.
Total Playback Duration (s)	Total playback duration of a video.
Total Requests	Total number of video playback requests.
Total Viewers	Total number of viewers.
Peak Viewers	Peak number of viewers.
Peak Bandwidth (bit/s)	Peak bandwidth consumed during playback.
Total Streaming Duration (s)	Total stream push duration.

Stream Push Monitoring

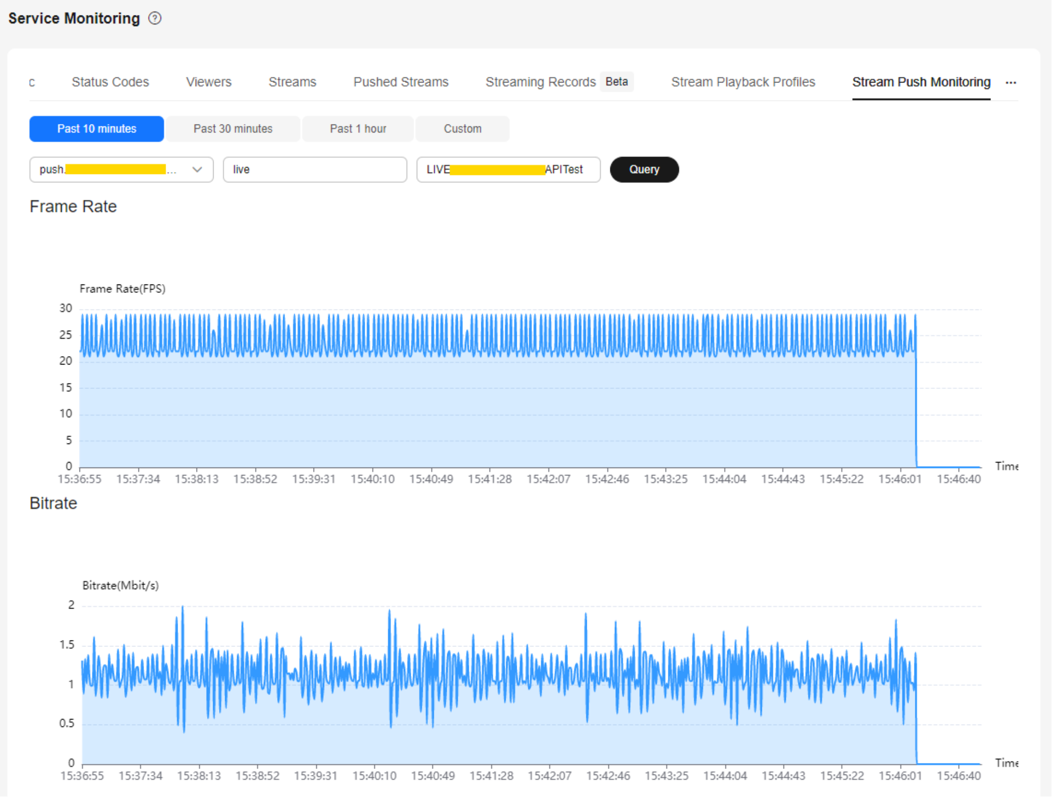
Specify the time, ingest domain name, app name, and stream name. Click **Query**. You can view related data in the **Frame Rate** and **Bitrate** areas.

NOTE

- You can query statistics of the past seven days.
- You can query statistics in a time span of up to 24 hours.

The **Frame Rate** and **Bitrate** areas display the trends of the frame rate and bitrate of livestreams (of the selected domain name) pushed to the origin server.

Figure 14-10 Frame rate/Bitrate statistics



Service Monitoring

push.[redacted]...

live

LIVE[redacted]APITest

15 Log Management

15.1 Offline Log Download

The offline log page displays detailed logs about the network users' access to all streaming domain names. You can download logs of a specific period to analyze the access to your service resources.

NOTICE

Log records are for data analysis and reference only. Service fees are charged based on bills.

Log Download

- You can download logs of the past 90 days.
- You can query and download logs in a time span of up to seven days. To query and download logs in a longer time span, perform the operations multiple times.

Log Description

Log package name format: *Streaming domain name_Log generation time*.log.gz

Log generation rule: By default, logs are collected at an interval of 5 minutes. If no request is sent to a domain name, no log data package is generated. Generally, the complete log file can be obtained four hours after the live stream push is completed.

Log format

- Cloud Stream Live

  [time_local]|play_domain|client_ip|cdn_ip|url|http_code|cache_hit|scheme|method|period_bytes_sent|period_duration|ua|refer|app|stream
- LLL

[time_local]|play_domain|client_ip|cdn_ip|url|http_code|cache_hit|scheme|method|period_bytes_sent|period_duration|ua|refer|app|stream

NOTE

If a field is not involved or is empty, the value of this field will be a hyphen (-). If the field information contains spaces, each space must be enclosed in double quotation marks ("").

Log example

- Cloud Stream Live
```
[06/Mar/2023:06:51:26 +0800]|pullexample.huaweicloud.com|49.1.1.*|42.11.1.2|http://
pullexample.huaweicloud.com/live/stream-123.flv|200|HIT|HTTP|GET|1024|4|Lavf/58.12.100|-|live|
stream-123
```
- LLL
```
[06/Mar/2023:06:51:26 +0800]|pullexample.huaweicloud.com|49.1.1.*|42.11.1.2|webrtc://
pullexample.huaweicloud.com/live/stream-123.sdp|200|HIT|WebRTC|GET|1024|4|Lavf/58.12.100|-|live|
stream-123
```

Table 15-1 describes the fields.

Table 15-1 Log fields

Field Name	Field Description	Example
time_local	Local time in the common format, which is used to record the time when statistics are collected.	[06/Mar/2023:06:51:26 +0800]
play_domain	Accelerated domain name added to CDN.	pullexample.huaweicloud.com
client_ip	IP address of the client.	49.1.1.*
cdn_ip	IP address of the CDN node accessed by the viewer.	42.11.1.2
url	Complete access URL.	• Cloud Stream Live http://pullexample.huaweicloud.com/live/stream-123.flv • LLL webrtc://pullexample.huaweicloud.com/live/stream-123.sdp
http_code	HTTP status code.	200
cache_hit	Cache hit status. • HIT • MISS	HIT

Field Name	Field Description	Example
scheme	Access protocol. ● HTTP ● HTTPS ● RTMP ● WebRTC	● Cloud Stream Live: HTTP, HTTPS, or RTMP ● LLL: WebRTC
method	HTTP method.	GET
period_bytes_sent	Number of bytes sent in a statistical period. The statistical period is the value of **period_duration**.	1024
period_duration	Statistical period, in seconds.	4
ua	User agent information.	Lavf/58.12.100
refer	Referer information.	-
app	App name	live
stream	Stream name	stream-123

Downloading Logs

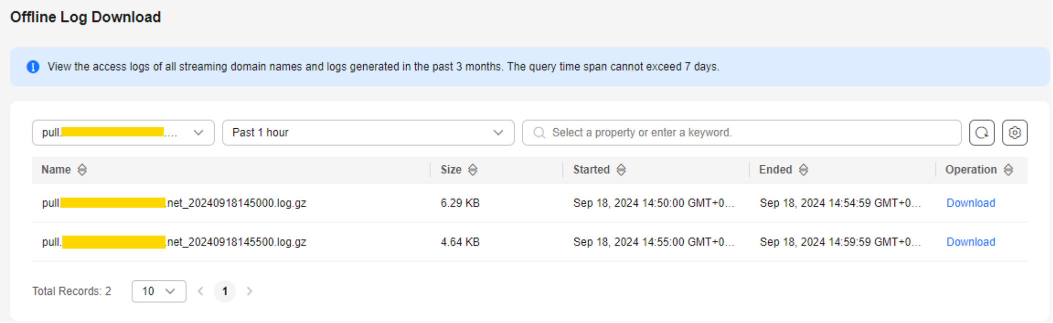
Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Logs** > **Offline log download**.

Step 3 On the displayed page, specify the domain name and time.

The system displays all logs generated in the specified time. A log file is generated every 5 minutes.

Figure 15-1 Downloading logs



Offline Log Download

View the access logs of all streaming domain names and logs generated in the past 3 months. The query time span cannot exceed 7 days.

pull.[redacted].... | Past 1 hour | Select a property or enter a keyword.

Name	Size	Started	Ended	Operation
pull[redacted].net_20240918145000.log.gz	6.29 KB	Sep 18, 2024 14:50:00 GMT+0...	Sep 18, 2024 14:54:59 GMT+0...	Download
pull.[redacted].net_20240918145500.log.gz	4.64 KB	Sep 18, 2024 14:55:00 GMT+0...	Sep 18, 2024 14:59:59 GMT+0...	Download

Total Records: 2 10 < 1 >

Step 4 Click **Download** in the **Operation** column in the row containing the log to be downloaded and download the log to your local PC.

----End

16 Tools

16.1 Signed URL Generation Tool

After configuring URL validation for an ingest domain name and a streaming domain name, you can use this tool to quickly generate signed URLs of the domain names.

Prerequisites

You have configured URL validation for your ingest and streaming domain names by referring to **Stream Authentication** and **URL Validation**.

Procedure

Step 1 Log in to the **Live console**.

Step 2 In the navigation pane, choose **Tools** > **URL Signing**.

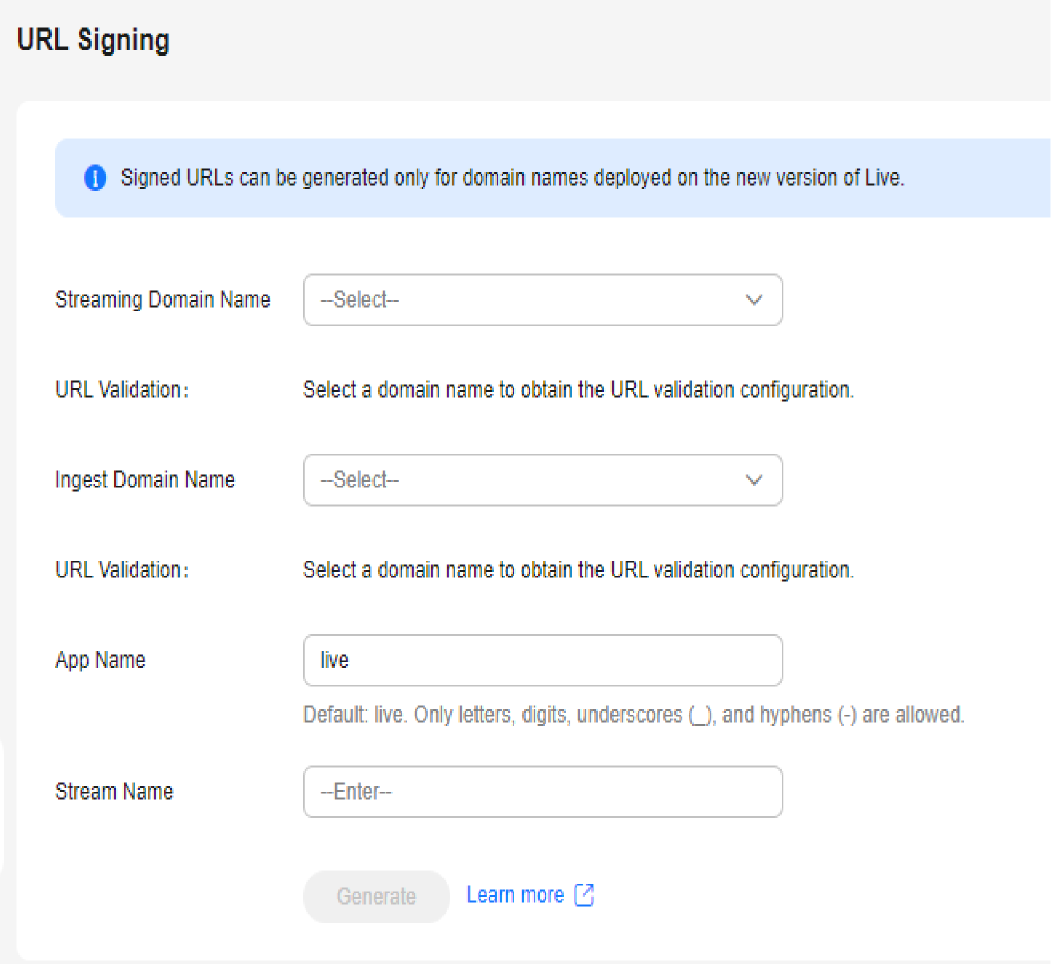
Step 3 Select the ingest domain name and streaming domain name for which a signed URL needs to be generated, and set **App Name** and **Stream Name**.

You can generate a signed URL only for the streaming domain name or ingest domain name.

NOTE

To generate a signed streaming URL after transcoding, set **Stream Name** to the value of *Stream Name_Transcoding template ID*, for example, **huawei01_lld**. You can obtain the transcoding template ID on the **Transcoding** page of the Live console.

Figure 16-1 Generating a signed URL



URL Signing

Signed URLs can be generated only for domain names deployed on the new version of Live.

Streaming Domain Name: --Select--

URL Validation: Select a domain name to obtain the URL validation configuration.

Ingest Domain Name: --Select--

URL Validation: Select a domain name to obtain the URL validation configuration.

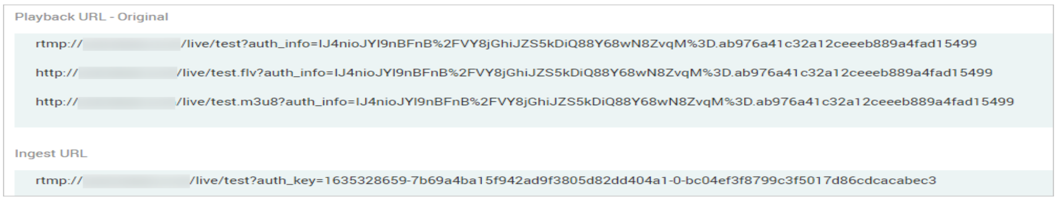
App Name: live

Default: live. Only letters, digits, underscores (_), and hyphens (-) are allowed.

Stream Name: --Enter--

Step 4 Click **Generate** to generate the signed ingest and streaming URLs.

Figure 16-2 Signed URLs



Playback URL - Original

```
rtmp://[redacted]/live/test?auth_info=IJ4nioJYI9nBFnB%2FVY8jGhiJZS5kDiQ88Y68wN8ZvqM%3D.ab976a41c32a12ceeeb889a4fad15499
http://[redacted]/live/test.flv?auth_info=IJ4nioJYI9nBFnB%2FVY8jGhiJZS5kDiQ88Y68wN8ZvqM%3D.ab976a41c32a12ceeeb889a4fad15499
http://[redacted]/live/test.m3u8?auth_info=IJ4nioJYI9nBFnB%2FVY8jGhiJZS5kDiQ88Y68wN8ZvqM%3D.ab976a41c32a12ceeeb889a4fad15499
```

Ingest URL

```
rtmp://[redacted]/live/test?auth_key=1635328659-7b69a4ba15f942ad9f3805d82dd404a1-0-bc04ef3f8799c3f5017d86cdcacabec3
```

----End