

Video on Demand

User Guide

Issue 01
Date 2026-04-10



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2026. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei 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 Prerequisites	1
2 Service Overview	2
3 Permissions Management	5
3.1 Creating a User and Assigning VOD Permissions	5
4 Domain Name Management	8
4.1 Configuring Domain Names	8
4.2 Configuring CNAME Records	13
4.3 Configuring IPv6 Access	16
4.4 HTTPS Settings	17
4.4.1 Overview	17
4.4.2 SCM Authorization	17
4.4.3 Configuring HTTPS Acceleration	19
4.4.4 HTTPS Certificate Requirements	22
4.5 Configuring Hotlink Protection	27
4.5.1 Referer Validation	27
4.5.2 URL Validation	30
4.6 Pseudo-Streaming	40
5 Audio/Video Upload	44
5.1 Overview	44
5.2 Local Upload	45
5.3 Pull from URLs (OBT)	46
6 Media Asset Management	49
6.1 Audio/Video Management	49
6.2 Cold Storage of Media Assets	59
6.2.1 Cold Storage Based on Media Asset ID	60
6.2.2 Intelligent Cold Storage Policies	61
7 Video Processing	64
7.1 Snapshot Capturing	64
7.2 Workflow Management	68
8 Global Settings	71

8.1 Transcoding Settings.....	71
8.2 Watermark Settings.....	81
8.3 Security Settings.....	83
8.3.1 HLS Encryption Settings.....	83
8.4 Tenant Settings.....	84
8.5 Authorizing Access to an OBS Bucket.....	85
8.6 Category Settings.....	85
8.7 Notifications.....	86
8.7.1 Overview.....	86
8.7.2 MFS.....	88
8.7.3 SMN.....	90
8.8 Workflow Settings.....	98
9 Review Management (in OBT).....	101
9.1 Enabling Content Moderation Authorization.....	101
9.2 Media Content Review.....	102
9.3 Review Settings.....	104
10 Usage Query.....	107
11 Data Analysis.....	113
11.1 Distribution Statistics.....	113
11.2 Playback Statistics.....	118
12 Task Center.....	121
13 Cloud Eye Monitoring.....	123
13.1 Monitoring Metrics.....	123
13.2 Creating an Alarm Rule.....	124
13.3 Viewing Monitoring Metrics.....	125
14 Querying Real-Time Traces.....	127
14.1 Key Operations Recorded by CTS.....	127
14.2 Viewing CTS Traces in the Trace List.....	130
15 Appendix.....	138
15.1 Permissions Management.....	138
15.1.1 Creating a User and Granting VOD Permissions.....	138
15.2 Obtaining a Project ID.....	140
15.3 Obtaining the AK/SK Pair.....	141
15.4 JSON Message Body.....	142
15.4.1 Transcoding Message Body.....	142
15.4.2 Snapshot Message Body.....	144
15.4.3 Review Message Body.....	145
15.4.4 Media Upload & Audio Extraction Message Body.....	149
15.4.5 Thumbnail Generation Message Body.....	151
15.4.6 Media Asset Parsing Message Body.....	152

15.4.7 Media Asset Editing Message Body.....	153
15.5 Installing JDK.....	153

1 Prerequisites

 **CAUTION**

- If you are a **Huawei Cloud (International)** user, you must 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 VOD in Huawei Cloud regions in the Chinese mainland.
- If you are a **Huawei Cloud (Chinese Mainland)** user, you must complete real-name authentication before purchasing and using VOD in regions outside the Chinese mainland.
- If your account is restricted, you are unable to purchase or use any VOD functions, including media asset upload, URL-based ingestion, media asset publishing, video snapshot management, and media asset transcoding.
- If you delete a project that had VOD enabled and then try to use VOD in a different project within the same region, you must re-enable VOD for that new project. This action does not affect any media files that already exist in that new project. For details about how to obtain a project ID, see [Obtaining a Project ID](#).
Deleting a project will also delete the media files and domain names associated with VOD in that project.
- If you have already enabled VOD (not through the VOD console) and the system displays a message indicating that you need to enable the service again, perform the operations below.

-
1. [Register a HUAWEI ID](#).
 2. Complete [real-name authentication](#).
 3. Top up your account (by at least \$0.15 USD) in [Billing Center](#).
 4. Log in to the [VOD console](#) and enable VOD as instructed.

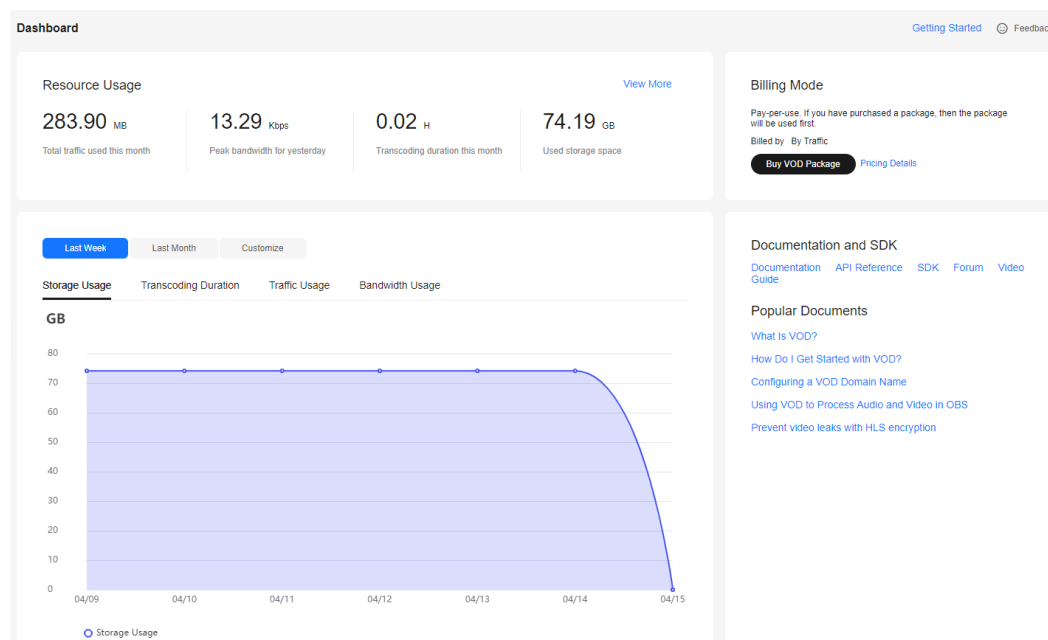
2 Service Overview

The VOD console provides functions such as audio and video upload and management, video processing, and audio and video moderation. You can view real-time monitoring information such as VOD resource usage and popular media assets on the console.

Dashboard

After you log in to the [VOD console](#), the **Dashboard** page is displayed. You can view the VOD resource usage and click **Getting Started** in the upper right corner for quick operation.

Figure 2-1 Dashboard



- You can view VOD resource usage in trend charts.

Table 2-1 Statistics

Item	Description
Storage Usage	<p>Storage space occupied by all media files, including input audio/video files, images, subtitles, and output media files.</p> <p>NOTICE There is a delay of at least one hour in obtaining storage space data. Only data for full-hour intervals is supported. Example:</p> <ul style="list-style-type: none"> • If the current Beijing time is 9:50, data from 7:00 to 8:00 can be obtained. • If the current Beijing time is 10:00, data from 8:00 to 9:00 can be obtained.
Transcoding Duration	<p>Total duration of transcoded videos (SD).</p> <ul style="list-style-type: none"> • For outputs in 4K or HD with the frame rate less than 30 fps, the duration is converted to SD-equivalent time using the ratios 4:2:1 (4K:HD:SD) for statistical purposes. • For outputs in 4K or HD with the frame rate greater than 30 fps, the duration is converted to SD-equivalent time using the ratios 5:2.5:1.25 (4K:HD:SD) for statistical purposes.
Traffic Usage	Total traffic used for VOD acceleration.
Bandwidth Usage	Daily peak bandwidth generated by VOD-accelerated content distribution.

- **Billing Mode** shows the current CDN billing mode. You can click **Change** to change the CDN billing mode.
The billing modes for distribution acceleration include by traffic, by daily peak bandwidth, and by 95th percentile bandwidth.
 - You cannot switch to the 95th percentile bandwidth billing mode on the console. To do so, you need to [submit a service ticket](#).
 - You cannot switch from the 95th percentile bandwidth billing mode to another mode on the console. To do so, you need to [submit a service ticket](#).
 - Only traffic-based billing is supported in the AP-Bangkok region, and the billing mode cannot be changed.

Functions

You can access various functions from the left navigation pane on the [VOD console](#).

Table 2-2 Console functions

Function	Description
Domain Name Management	You can add and manage your own domain names, and configure HTTPS and hotlink protection for these domains.
Audio/Video Upload	You can upload audio/video files from the local PC, or pull audio/video files from their URLs.
Audio/Video Management	You can perform operations on uploaded audio/video files, including transcoding, real-time container format conversion, pre-loading and updating media asset information on CDN, canceling transcoding, restoring archived files, changing the storage class, categorizing media assets, extracting audio, exporting media asset information, deleting media assets, viewing basic information of media assets, and obtaining media asset streaming URLs.
Video Processing	You can perform operations on video files, such as snapshot capturing and workflow creation.
Global Settings	You can configure transcoding templates, watermark templates, HLS encryption, tenant-level media asset cold storage, categories, event notifications, and workflows.
Audio/Video Review	Audios, images, and files can be automatically or manually reviewed to block inappropriate content. NOTE This function is not available in AP-Bangkok.
Usage Query	You can view the traffic and peak bandwidth statistics on CDN, as well as the storage space and transcoding duration used on the VOD origin server.
Data Analysis	You can view data such as the traffic, bandwidth, and traffic hit ratio on CDN, as well as the number of playback times and ranking (by playback times) of audio/video files by domain name.

3 Permissions Management

3.1 Creating a User and Assigning VOD Permissions

This section describes how to use [IAM](#) to implement fine-grained permissions management on your VOD resources. With IAM, you can:

- With IAM, you can create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own identity credentials for accessing VOD resources.
- Assign users only the permissions required to perform a given task based on their job responsibilities.
- Entrust a Huawei Cloud account or cloud service to perform efficient O&M on your VOD resources.

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

This section describes the process of assigning permissions (see [Figure 3-1](#)).

Prerequisites

Learn about the permissions (see [Permissions Management](#)) supported by VOD and choose policies or roles according to your requirements.

Notes

As of December 30, 2024, policies will be the only way to manage VOD permissions. Policies are easy to configure and allow flexible permission settings, meeting your requirements for IAM user permissions management in different scenarios.

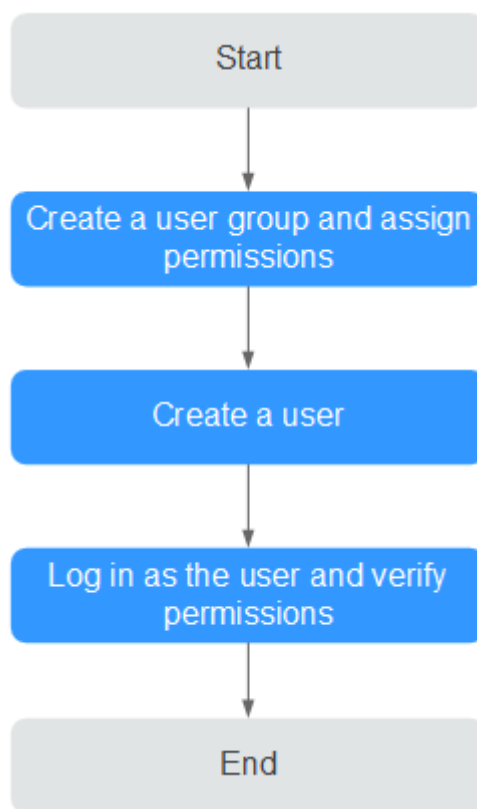
NOTICE

If you enabled VOD before December 30, 2024 and are using both roles and policies to manage VOD permissions, you can continue with the approach. For details, see [Creating a User and Granting VOD Permissions](#).

To switch to the policy-only approach for VOD permissions management, [submit a service ticket](#).

Process Flow

Figure 3-1 Process of assigning VOD read-only permissions



1. **Create a user group and assign permissions.**
Create a user group on the IAM console and attach the **VOD ReadOnlyAccess** policy to the group.
2. **Create an IAM user and add it to the user group.**
Create a user on the IAM console and add it to the group created in **1**.
3. **Log in** as the IAM user and verify permissions.
In the authorized region, perform the following operations:
 - Choose **Service List > Video on Demand**. The VOD console is displayed. If a message is displayed indicating insufficient permissions for performing the operation, the **ReadOnlyAccess** policy has already taken effect.

- Choose any other service in **Service List**. If a message is displayed indicating insufficient permissions for the service, the **VOD ReadOnlyAccess** policy has already taken effect.

4 Domain Name Management

4.1 Configuring Domain Names

You can use your own domain names to accelerate media distribution.

NOTICE

- All domain names of the system have been assigned. If you do not have an assigned domain name after subscribing to VOD, you need to add licensed domain names to VOD for media distribution acceleration.
 - System-assigned domain names will be unavailable on June 30, 2026. If you are using system-assigned domain names, switch to your own domain names before June 30, 2026 to continue using VOD.
-

Notes

- If you have **enabled** the Enterprise Project Management Service (EPS), you can add domain names to enterprise projects for easy management. You can use the default enterprise project **default** or create your own by referring to [Creating an Enterprise Project](#).
- The system automatically checks all domain names under your name and disables or deletes those that have been idle for a long time.
 - Disabling a domain name: If a domain name generates no downstream traffic for one month, it will be automatically disabled and displayed in the **Disabled** status on the VOD console.
 - Deleting a domain name: If a domain name generates no downstream traffic for two months, it will be deleted.
- After a domain name is disabled or deleted, it can no longer be used to distribute or play media files, but it can still be used to upload or process media files.

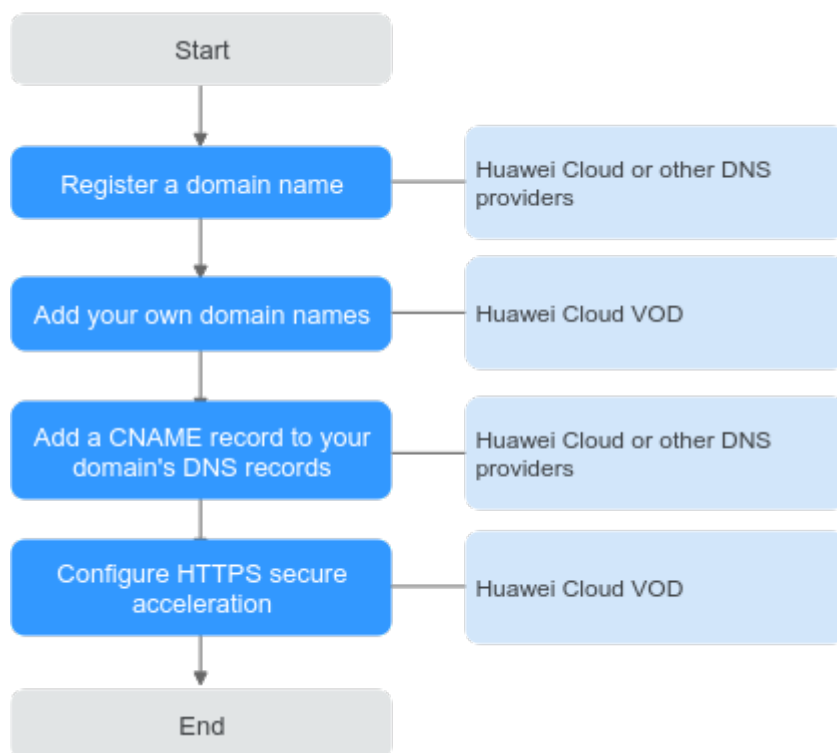
If a domain name is in an abnormal state, such as being disabled, the CDN cache cannot be cleared when you delete media assets. After the domain name becomes normal again, you must manually trigger the cache clearing operation.

- Restoring a domain name: If a domain name is disabled, you can manually enable it on the **Domain Name Management** page of the VOD console. If a domain name has been deleted, you need to add the domain name again and configure its CNAME record before it can be used. System-allocated acceleration domain names (provided upon VOD subscription) cannot be restored once deleted.
- When you delete a domain name that has been idle for more than half a year, an error will be reported. In this case, you need to [submit a service ticket](#) for assistance.

Domain Admission Process

Figure 4-1 shows the process of using your own domain names for VOD acceleration.

Figure 4-1 Domain admission process



1. Register a domain name. If you do not have a domain name, you can purchase or register a domain name with the cloud service provider.
2. Add your domain names to VOD. Up to five domain names can be added. For details, see [Adding Domain Names](#).
3. Add a CNAME record to your domain's DNS records. For details, see [Configuring CNAME Records](#).
4. Configure HTTPS secure acceleration. VOD content is streamed over HTTPS by default, so you need to upload an HTTPS certificate for your domain name. Otherwise, the uploaded media files cannot be played. For details, see [Configuring HTTPS Secure Acceleration](#).

 **NOTE**

After your domain name is added, VOD will review the content distributed through the domain. If any content is found to violate applicable laws or regulations, for example, pornography-, gambling-, or drug-related content, the domain's resolution will be terminated.

Adding Domain Names

Step 1 Log in to the [VOD console](#).

Step 2 In the navigation pane, choose **Domain Name Management**.

Step 3 Click **Add Domain Name**. The **Add Domain Name** page is displayed.

[Table 4-1](#) describes the required parameters.

Table 4-1 Adding a domain name

Parameter	Description
Domain Name	<p>Enter a licensed domain name.</p> <ul style="list-style-type: none"> You can add a maximum of five domain names. Wildcard domains such as *.example.com are not allowed. You are advised to use a third-level or deeper domain name, for example, example.yourdomain.com.
Enterprise Project	<p>If you have enabled the Enterprise Project Management Service (EPS), you need to select an enterprise project for easy domain management.</p>
Service Scope	<p>Service scope of the current domain name.</p> <p>The options are as follows:</p> <ul style="list-style-type: none"> Chinese mainland: Only users in the Chinese mainland can access the VOD content of the current domain name. Outside China: Only users outside the Chinese mainland can access the VOD content of the current domain name. Global: Global users can access the VOD content of the current domain name. <p>NOTICE If the Service Scope 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 Service Agreement.</p>

Step 4 Click **OK**.

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

After a domain name is added, the system assigns a CNAME value to the domain name.

Step 5 Add a CNAME record to your domain's DNS records by referring to [Configuring CNAME Records](#) and verify whether the CNAME record has taken effect.

Since the domain is enabled by default after being added to VOD, if the CNAME record is not configured, VOD media playback may fail and thumbnails may not display.

Step 6 Click **Set as Default** next to the domain you added to make it the default domain.

Each account can only have one default domain in the **Enabled** state. You need to enable [HTTPS acceleration](#) for the domain name and upload the HTTPS certificate so that the domain name can be used to provide VOD services.

----End

Managing Domain Names

After a self-owned domain name is added, you can view basic information about the domain name on the **Domain Name Management** page. You can also disable, enable, or delete the domain name. If you have [enabled](#) the enterprise project management service, you can also view the name of the enterprise project to which a domain name belongs.

Step 1 Log in to the [VOD console](#).

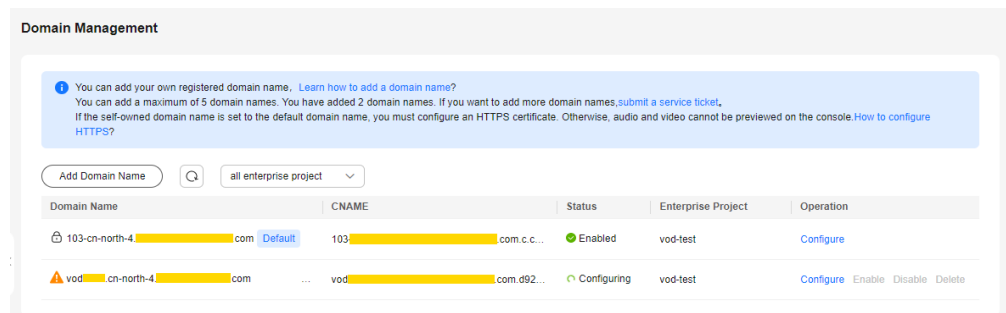
Step 2 In the navigation pane, choose **Domain Name Management**.

Step 3 You can perform the following operations as required:

- Viewing domain information

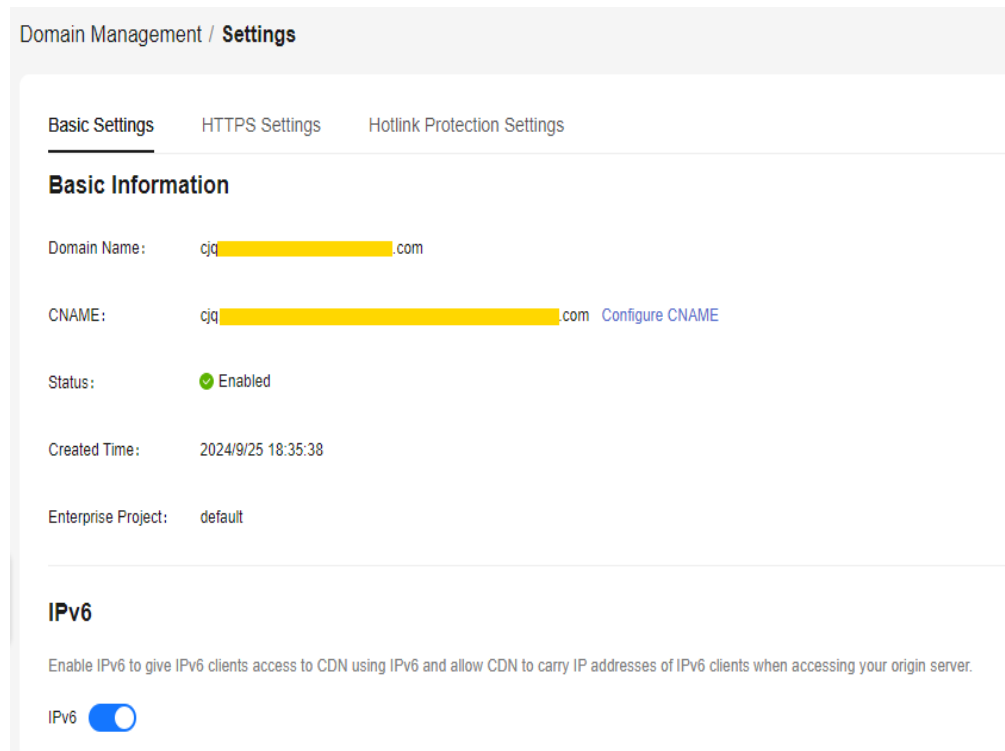
In the domain name list, you can view the CNAME value and status of the added domain name.

Figure 4-2 Domain information



Click **Configure** in the **Operation** column on the right to view the basic configuration of the target domain name. You can also configure [HTTPS secure acceleration](#) and [Referer validation](#) for the domain name.

Figure 4-3 Domain name security configuration



- Disabling 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.

NOTE

Ensure that the default domain name has been enabled. Otherwise, media file playback will fail.

- Enabling a domain name
To enable a disabled domain name, click **Enable** in the **Operation** column. If the **Status** changes to **Enabled**, the domain name has been enabled.
- Deleting 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.
When you delete a domain name that has been idle for more than half a year, an error will be reported. In this case, you need to [submit a service ticket](#) for assistance.

----End

Follow-up Operations

After the domain name is added, you can configure the domain name on the VOD console. The details are as follows:

- [Configure HTTPS secure acceleration](#) to ensure that VOD media files are encrypted during transmission.

- **Configure referer validation** to identify the request source by the referer field carried in a playback request and filter out unauthorized requests.
- **Configure URL validation** to prevent resources uploaded by subscribers to the VOD service from being stolen.

4.2 Configuring CNAME Records

After a domain name is added, the system automatically assigns a CNAME value to the domain name. You need to add the CNAME record to your domain's DNS records. Acceleration is enabled once the configuration takes effect.

Notes

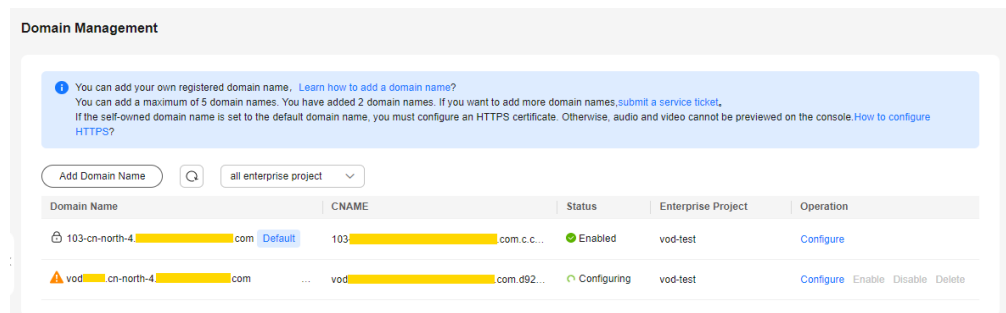
- If your domain name is not registered on the Huawei Cloud Domain Registration Service, configure the CNAME record following the guidance provided by your DNS service provider.

Procedure

Step 1 Obtain the CNAME record.

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

Figure 4-4 Domain information

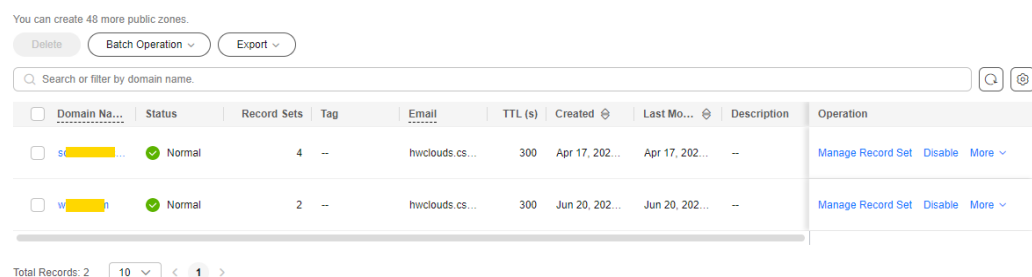


Step 2 Log in to the **DNS console**.

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 4-5**.

Figure 4-5 Domain name list



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

Figure 4-6 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: --

Cancel OK

Configure the parameters by referring to [Table 4-2](#).

Table 4-2 Parameters

Parameter	Description
Type	Type of the record set. Select CNAME – Map one domain to another here.
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)	How long a local DNS server caches the DNS record. It is measured in seconds. The smaller the value is, the quicker the record takes effect. The default value is 300 seconds. You can retain the default value.
Value	Domain name to be pointed to, that is, the CNAME address 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. <ul style="list-style-type: none"> • 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 implement weighted routing by setting different weights for them. For details, see Configuring Weighted Routing . 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: <ul style="list-style-type: none"> • example_key1 • example_value1

Parameter	Description
Description	(Optional) Supplementary information about the domain name. You can enter up to 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.

----End

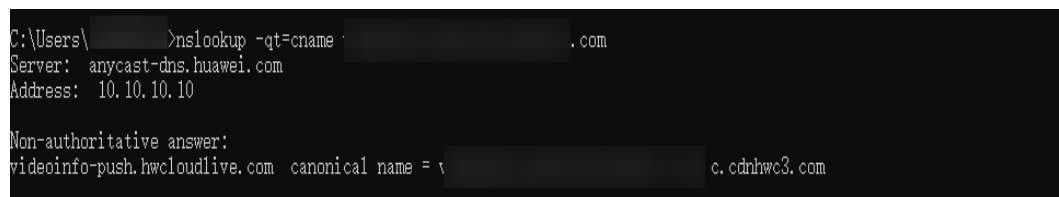
Verifying that the CNAME Has Taken Effect

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

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

If the CNAME is displayed, the CNAME has taken effect. A typical command output is shown in [Figure 4-7](#).

Figure 4-7 Command output



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

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

4.3 Configuring IPv6 Access

After IPv6 is enabled, the IPv6-compatible client can access the VOD service using the IPv6 protocol.

Notes


After IPv6 is enabled, if IPv6 is used to access VOD but the optimal node does not support IPv6, VOD can still be accessed using IPv4.

Procedure

- Step 1** Log in to the [VOD console](#).
- Step 2** In the navigation pane, choose **Domain Name Management**.
- Step 3** In the **Operation** column of the desired domain name, click **Configure**.
- Step 4** In the **IPv6** area, enable **IPv6**, as shown in [Figure 4-8](#).

Figure 4-8 IPv6**IPv6**

Enable IPv6 to give IPv6 clients access to CDN using IPv6 and allow CDN to carry IP addresses of IPv6 clients when accessing your origin server.

IPv6 

----End

4.4 HTTPS Settings

4.4.1 Overview

HTTPS ensures secure transmission through encryption and identity authentication. It is widely used in security-sensitive web communications, such as online payments.

- You can configure an HTTPS certificate for your domain name so that VOD can serve content over HTTPS. Clients can then access VOD content via HTTPS.
- Before modifying the certificate settings of a domain name, ensure that:
 - The domain name is in the **Enabled** or **Configuring** state and is not locked or banned.
 - The HTTPS certificate is not in the **Configuring** state.

Function	Description
SCM Authorization	To configure SCM certificates in VOD, you must first set up an SCM agency. This allows you to directly obtain certificate content during configuration.
Configuring HTTPS Acceleration	Adding an HTTPS certificate for your domain in VOD allows clients to access your content securely via HTTPS.
HTTPS Certificate Requirements	Combining and uploading certificates issued by different authorities must follow the specific rules.

4.4.2 SCM Authorization

If your certificate has been uploaded to **Cloud Certificate & Manager (CCM)** of Huawei Cloud, you can enable SCM authorization so that you can directly select the certificate on the VOD console.

Constraints

1. IAM users can enable SCM authorization only when they have the permissions below.

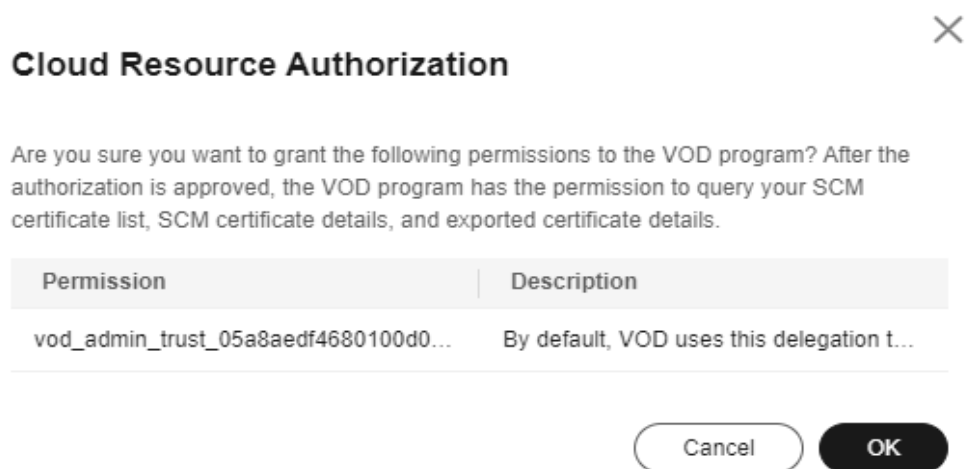
Related Cloud Service	Permission
IAM	<ul style="list-style-type: none"> • iam:roles:listRoles • iam:roles:createRole • iam:agencies:listAgencies • iam:agencies:createAgency • iam:permissions:checkRoleForAgency • iam:permissions:grantRoleToAgency

2. After creating an agency, IAM users can configure certificates for domain names when they have the following permissions:
 - vod:domain:modifyHttpsSetting
 - vod:domain:getHttpsSetting
 - vod:domain:list

Enabling SCM Authorization

- Step 1** Log in to the [VOD console](#).
- Step 2** In the navigation pane, choose **Domain Name Management**.
- Step 3** In the upper right corner of the page, click **Enable SCM Authorization**.

Figure 4-9 Cloud resource authorization



- Step 4** Click **OK**.

The system creates an agency named **vod_admin_trust_{domain_ID}** on the **Agencies** page of the **IAM console**. VOD now has the permissions to list your SCM certificates, query SCM certificate details, and export certificate details.

 **NOTE**

Do not delete this agency. Otherwise, VOD cannot obtain certificate content when you configure an HTTPS certificate.

----End

4.4.3 Configuring HTTPS Acceleration

Configuring HTTPS acceleration helps protect your VOD resources. HTTPS is enabled by default for domain names allocated by VOD. If you use your own domain name for VOD acceleration, you must manually enable HTTPS. Without HTTPS enabled, previewing and playing media files on the VOD console will not be possible.

Background

Forcible Direction to HTTPS: After configuring an HTTPS certificate, you can optionally enable **Forcible Direction to HTTPS**. When enabled, the server returns a 302 response to HTTP requests and redirects users to HTTPS.

HTTP 2.0: The HTTP/2 specification was published as RFC 7540 in May 2015. The standardization effort was supported by Chrome, Opera, Firefox, Internet Explorer 11, Safari, Amazon Silk, and Edge browsers.

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 tampered with during transmission, ensuring data integrity.
- Key user information is encrypted to prevent session IDs or cookies from being captured by attackers.

HTTP/2 has the following advantages:

- Multiplexing: Multiple HTTP requests can be sent and responses can be received asynchronously via a single TCP connection.
- Binary framing: All HTTP/2 communication is split into smaller messages and frames, each of which is encoded in binary format to replace plaintext transmission in HTTP/1.x.
- Server push: A server can actively push responses into client caches, speeding up web page loading.
- Header compression: HTTP/2 uses the HPACK algorithm designed for header compression. It compresses the message header and creates an index table for the message header. For the same message header, only the index number is sent, reducing the transmission of header data.

Prerequisites

- A domain name has been configured. For details, see [Configuring Domain Names](#).

- The HTTPS certificate has been prepared. If no HTTPS certificate is available, access the [SSL Certificate Manager](#) to buy an HTTPS certificate.
- 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

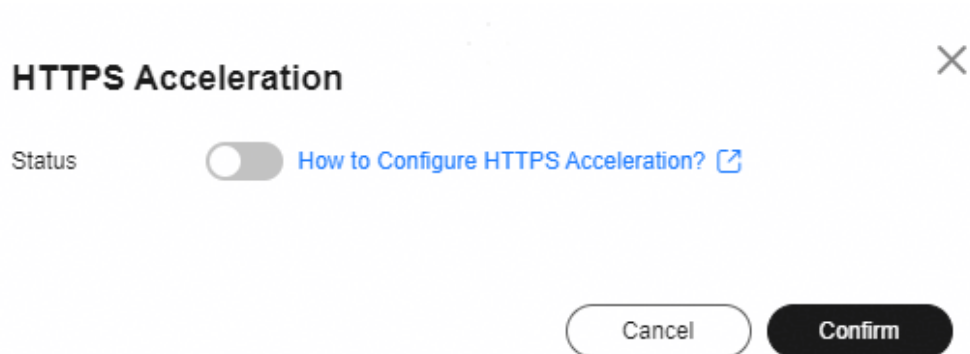
Step 1 Log in to the [VOD console](#).

Step 2 In the navigation pane, choose **Domain Name Management**.

Step 3 Locate your domain name and click **Configure** in the **Operation** column. On the displayed page, select the **HTTPS Settings** tab.

Step 4 Click **Edit** on the right of **HTTPS Settings**. The **HTTPS Acceleration** dialog box is displayed, as shown in [Figure 4-10](#).

Figure 4-10 Enabling HTTPS acceleration



Step 5 Turn on the switch and set HTTPS parameters shown in [Figure 4-11](#).

For details about parameter settings, see [Table 4-3](#).

Figure 4-11 Configuring an HTTPS certificate

HTTPS Acceleration ✕

Status [How to Configure HTTPS Acceleration?](#)

Certificate Source Self-owned Certificate SCM Certificate


Certificate Name

Certificate Body

Private Key

Table 4-3 Certificate settings

Parameter	Description
Certificate Source	Source of the HTTPS certificate. Options: <ul style="list-style-type: none">• Self-owned Certificate• SCM Certificate

Parameter	Description
Self-owned certificate settings	<p>Set the certificate name, use a text editor to open the obtained certificate file and private key file, and copy the content to the Certificate Body and Private Key text boxes. Certificates issued by different organizations are different:</p> <ul style="list-style-type: none"> If your certificate is issued by the root CA, the certificate is a complete certificate. Copy the certificate content. <p>Figure 4-12 HTTPS certificate</p>  <ul style="list-style-type: none"> 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. For details, see Certificates Issued by Intermediate CAs.
SCM certificate settings	VOD automatically obtains SSL certificates uploaded to the CCM console. You only need to select the desired one from the drop-down list.

Step 6 Select whether to enable **Forcible Redirection to HTTPS** and **HTTP2.0**.

- Forcible Redirection to HTTPS:** If this function is enabled, all requests for accessing media in VOD are forcibly redirected to HTTPS.
- HTTP2.0:** If this function is enabled, all requests for accessing media in VOD comply with the HTTP/2 protocol.

Step 7 Verify whether HTTPS secure acceleration has taken effect.

If the playback URL begins with https:// and the audio or video plays successfully from that URL, HTTPS secure acceleration has taken effect.

----End

Updating a Certificate

If your certificate is about to expire or has been revoked, you need to synchronize the new certificate to the HTTPS settings. The procedure of updating a certificate is the same as that of [enabling HTTPS](#).

4.4.4 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.

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

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

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

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

Figure 4-14 A combined certificate

```
-----BEGIN CERTIFICATE-----
MIIE/DCCA+SgAwIBAgIUOWwvEj41j5OamNabjVbGY42BBcQwDQYJKoZIhvcNAQEL
BQAwYIxCzAJBgNVBAYTAmNuMRIwEAYDVQQIDAlHdWFuZ0RvbmNlcjEAPBgNVBAcM
CFNoZW56aGVuMQ8wDQYDVQQKDAZidWF3ZWkxZCZAJBgNVBAsMAk1UMS4wLWVhZDQw
DCVidWF3ZWkxZDViIFN1Y3VyZSBjbnR1cm5ldCBHYXR1d2F5IENBMB4XDTE3MTAx
ODAwNDA0N1oXDTE4MTAxODAwNDA0N1owZz0xZCZAJBgNVBAYTAKNOMRAwDgYDVQQI
DAdqawFuZ3N1MRawDgYDVQQHDAduYW5qaW5nMS4wLWVhZDQwDQYDVQIDWF3ZWkxZDQw
dHdhcmUgVGVjaG5vbG9naWVzIENvLiVhZDQwDQYDVQIDBDBDBG91ZGJ1IFNS
RSBEZXBOMRwwGgYDVQQDDBN3d3cuaHVhd2VpY2xvdWQuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA3f5hC6J20XSF/Y7Wb8o6130yzgaUYWGLEX8t
1dQ1JAus93xMC2Jr6UOXmXR6WaRu51ZxpPFLT/IV6UnvMLnxJQBavqauykCskadW
stYA9ttTI/FYq+MR1XKbNrqK/ADhrfmR4owS/3w1wxdpwy5TRZ+V/D6TjxHZCjc
+81SmUuLxsgoUe79B/ruccY1ufuqr3v0TToaNN4c37kwjJeKf+b2F/IqO/KF+9zF
AgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMEIGA1UdEQQ7MDmCE3d3dy5odWF3ZW1j
bG91ZC5jb22CESouaHVhd2VpY2xvdWQuY29tgg9odWF3ZW1jbG91ZC5jb20wDQYJ
KoZIhvcNAQELBQADggEBACsLP7Hj+4KY1ES38OnOWuwQ3st8axvhDD9jZGoninzW
JSGpdm04NEshlvSfDEHpy/xKSLCIqg5Ue8tTI8zOF13U0ROnMeHKSXsJG6zc8X
h/3N217oBygPgvpmc6YX66kvwXmbA7KRniYS0nmCi2KUyng5Bv4dsx21djlqQ3b
HI+i026Q9odLsmhsKOsFUC0vDKoMIJz0Socy7Cq1+tFWF9S79MI4QjxaXVEvpIEg
QLEze3BXSsoiWRkdfsDB9s+UtdWeJy0HMh/otwUQQtB6areV2+CPthfmDENA+A8
IK6GzHyp/mgrwKdDh97aQ42ARreAv4KVFAiJGZ02LOY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID2CCAsGgAwIBAgIJALQPO9XxFFZmMA0GCSqGSIb3DQEBwUAMIGCMQswCQYD
VQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25nMREwDwYDVQQHDAhTaGVuemhlbjEP
MA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDLDAJVVDEuMCwGA1UEAw1SHVhd2VpIFdl
YiBTZWN1cmUgSW50ZXJuzXQgR2F0ZXdheSBDQTAeFw0xNjA1MTAwOTAyMjdaFw0y
NjA1MDgwOTAyMjdaMIGCMQswCQYDVQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25n
MREwDwYDVQQHDAhTaGVuemhlbjEPMA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDLDAJ
VDEuMCwGA1UEAw1SHVhd2VpIFdlYiBTZWN1cmUgSW50ZXJuzXQgR2F0ZXdheSBD
rG0CAwEAAaNQME4wHQYDVRO0BBYEFDB6DZX4Am+isCoa48e4ZdrAXpsMB8GA1Ud
IwQYMBaAFDB6DZX4Am+isCoa48e4ZdrAXpsMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAKN9ksjRX56yw2Ku5Mm3gzU/kQQw+mLkIuJEeDwS6LWjW0Hv
313xlv/Uxw4hQmo6OXqQ2OM4dfIJoVYKqilLlBCpXvO/X600rq3UPediEMaXkmM+F
tuJnoPCXmew7QvvQQvwis+0xmhpRPg0N6xIK01vIbAV69TkpWJW3duj1FuRjGsvn
rRab4gVi14x+bUgTb6HCvDH99PhADvXOuI1mk6Kb/JhCNbhrAHezyfLrvimxIOKy
2KZWitN+M1UWvSYG8jmtDm+/FuA93V1yErRjKj92egCgMlu671liddt7zzzzqW+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 4-15](#).

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 4-15 An RSA private key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAxDKJJ/hArR+Sq2YyqOWUN2Jh822dGcexU58g909eY1vLCqow
wEPqs6vyqQM3gKo8qCkNkmS5QgMPOFI4fx2G22mHvT0x8PHjm6GTQDPDniWaIuky
lufqVPD/zqK0oBl2AeAvbzKxWwRqf4JTLA3136B415y2VoDjRfU5EKY6LW1sD/00
5uF0qE3td5KQwQc6ZzbnkAof0Oyp5PbMfajM9My2mcvQJzWPLRxET3eWHYdBUtEg
1rxdrWxLheKjENzW3P7Mz/7KycIRxAlur1/Z9s8ytj3124AQY7NE1t1iL9wwA47k
0EumxTaLz8H/vHB1fLMouvYfsSDEr3Snf6eSSwIDAQABAoIBAQCDCNmxC3qHXPgvI
EzBOtIPVl1PyzizXWi+U4U6WwUBjCQ6ijfoYOKLaHHnnCEIm4V2N8KV4prAkQjcm
-----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
```

4.5 Configuring Hotlink Protection

4.5.1 Referrer Validation

Referer validation allows you to control access sources based on the referer field carried in a request. CDN filters requests based on the configured blacklist or whitelist.

Notes

- This function is optional and is disabled by default.
- Whitelists and blacklists cannot be used simultaneously.
- A maximum of 100 domain names, each with up to four levels, can be added to the blacklist or whitelist.
- Domain names added to a blacklist or whitelist cannot include protocol names. Domain names are matched by prefix. For example, if **^example.example*.com\$** is entered, both **example.example.com** and **example.example01.com** are matched.
- Domain names with ports cannot be added to referer whitelists or blacklists.

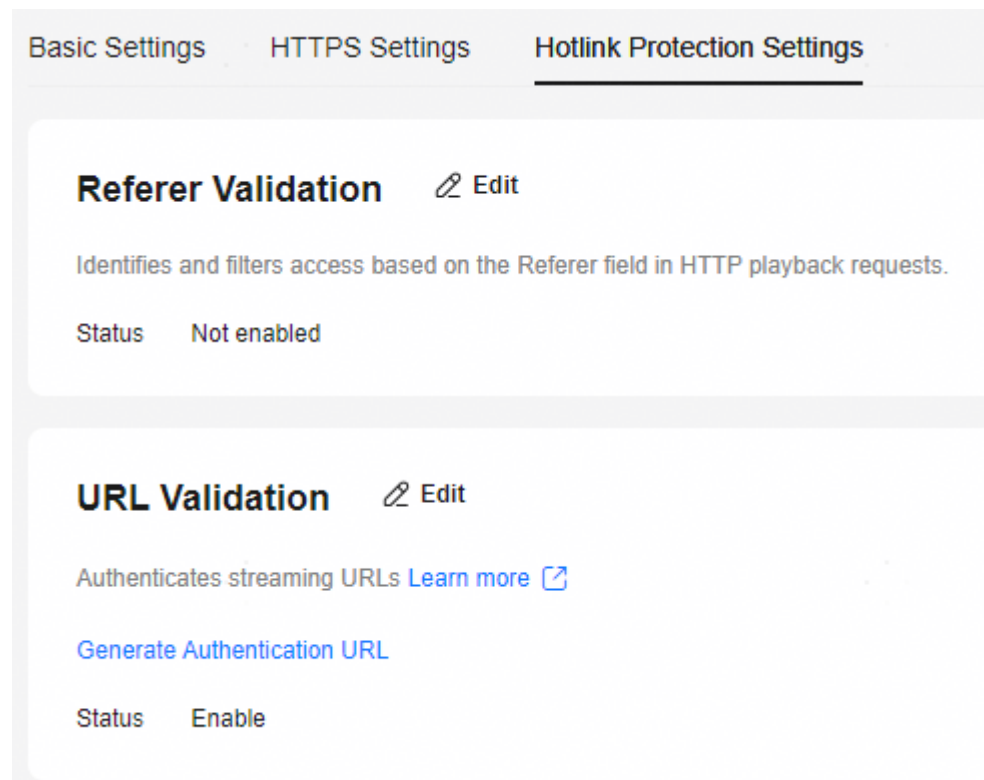
Procedure

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

Step 2 In the navigation pane, choose **Domain Name Management**.

Step 3 Locate the desired domain name and click **Configure** in the **Operation** column. On the displayed page, choose the **Hotlink Protection Settings** tab.

Figure 4-16 Hotlink protection settings



Step 4 Click **Edit** on the right of **Referer Validation**. The **Referer Validation** dialog box is displayed, as shown in [Figure 4-17](#).

Configure referer validation parameters by referring to [Table 4-4](#).

Figure 4-17 Referrer validation settings

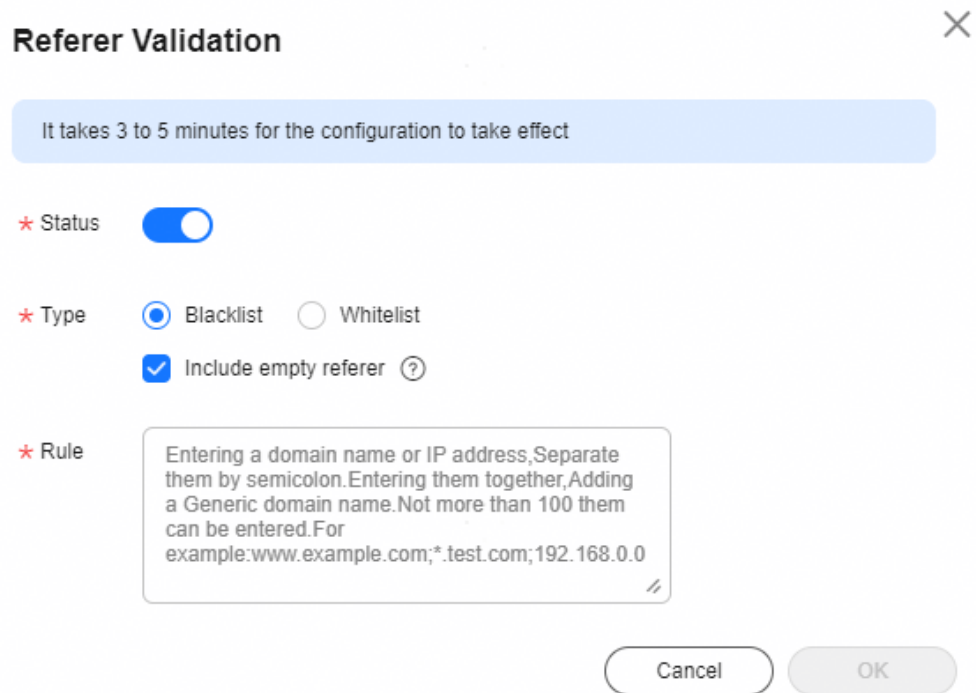


Table 4-4 Parameters

Parameter	Description
Status	Whether to enable referer validation. By default, referer validation is enabled.
Type	Blacklists and whitelists are supported. <ul style="list-style-type: none"> • Blacklist: Domains on the blacklist are blocked from accessing VOD resources. All other domains are allowed. If Include empty referer is selected, requests with empty referer in the HTTP header are also blocked. • Whitelist: Only domains on the whitelist are allowed to access VOD resources. All other domains are blocked. If Include empty referer is selected, requests with empty referer in the HTTP header are also allowed.
Rule	Domain names in the blacklist or whitelist. Domain names and IP addresses can be input at the same time and separated with semicolons (;). Wildcard domain names are allowed. A maximum of 100 domain names and IP addresses in total can be entered. Example: www.example.com;*.test.com;192.168.0.0

Step 5 Click **OK**.

It takes about 3 to 5 minutes for the referer validation settings to take effect.

----End

4.5.2 URL Validation

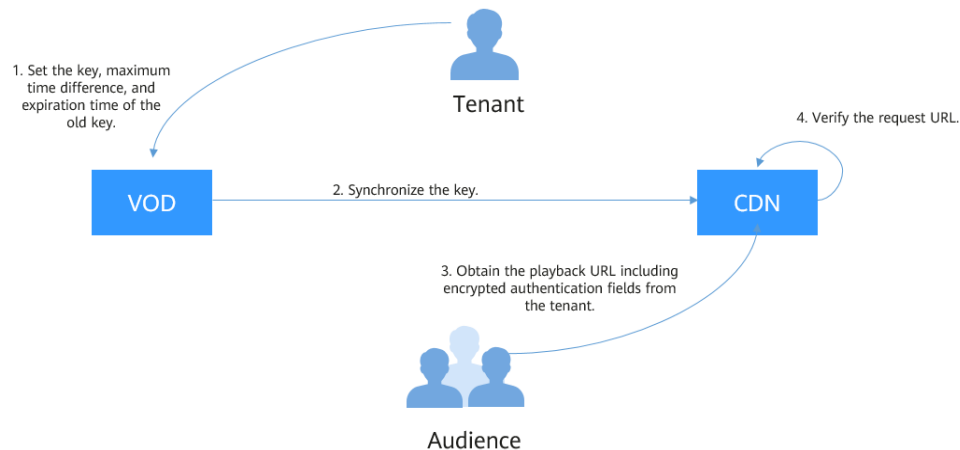
Referer validation can filter requests by checking the HTTP referer header. However, the referer header can be forged, so referer validation cannot fully protect your VOD resources. For better protection, VOD provides URL validation. You can configure a key to generate signed playback URLs with an expiration time. This method effectively prevents your VOD content from being illegally accessed.

Implementation

Referer validation works in a simple way. After a blacklist or whitelist is configured on the VOD console, VOD distributes the blacklist or whitelist to CDN. When receiving a request, CDN checks whether the request is valid based on the list. If the request is valid, CDN accesses the requested resource. If the request is invalid, CDN rejects the request and returns a status code 403.

URL validation is implemented by VOD edge nodes and origin server in VOD. It is a more secure and reliable anti-piracy solution than referer validation. [Figure 4-18](#) shows how URL validation works.

Figure 4-18 URL validation working principles



The process is as follows:

1. You enable URL validation on the VOD console and configure the allowed time difference and algorithm.
2. VOD delivers the configured key value to CDN nodes.
3. You obtain the authentication URL of a VOD media file.
4. Viewers request CDN to play a video through the authentication playback URL.
5. CDN verifies the request based on authentication information carried in the playback URL. Only requests that pass the verification are allowed.

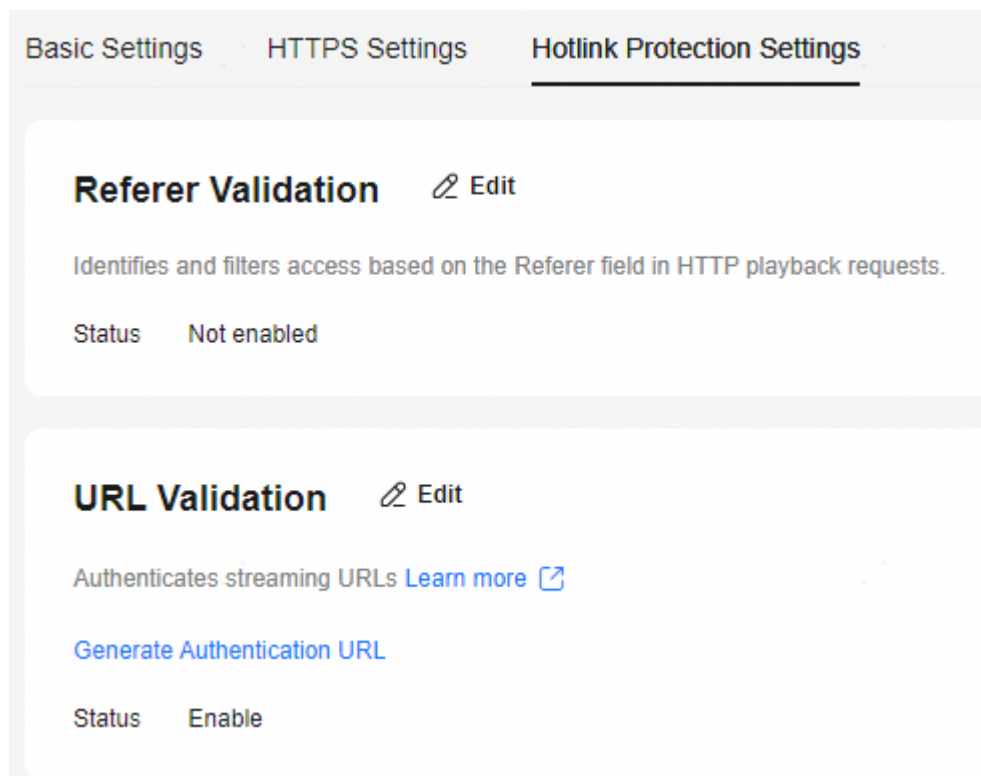
Notes

- This function is optional and is disabled by default.
- After this function is enabled, the original URLs can no longer be used. You must generate new signed URLs based on the configured rules.
- If a signed URL expires or the signature fails verification, playback will be blocked, and a "403 Forbidden" error will be returned.
- Algorithms A, B, and C do not support HLS or DASH playback. Algorithm E is recommended.
- Algorithms A, B, C, and D are insecure. Algorithm E is recommended.
- When URL validation is enabled, playback with multiple audio tracks and multilingual subtitles is not supported.

Procedure

- Step 1** Log in to the [VOD console](#).
- Step 2** In the navigation pane, choose **Domain Name Management**.
- Step 3** Locate the desired domain name and click **Configure** in the **Operation** column. On the displayed page, choose the **Hotlink Protection Settings** tab.

Figure 4-19 Hotlink protection settings



- Step 4** Click **Edit** on the right of **URL Validation**. The **URL Validation** dialog box is displayed, as shown in [Figure 4-20](#).

Configure URL validation settings based on [Table 4-5](#).

Figure 4-20 Configuring URL validation

URL Validation ✕

1. Algorithm ABCD are historically insecure algorithms. It is recommended that users choose Algorithm E.

2. Algorithm E is recommended in the real-time encapsulation scenario. For DASH, only the primary index can be authenticated. The authentication scope cannot be all files.

Status

* Signing Key ? 👁 Generate

You are advised to click the button on the right to generate the key. If the key is not random enough, the security of the authentication information cannot be ensured.

Secondary Key 👁 Generate

You are advised to click the button on the right to generate the key. If the key is not random enough, the security of the authentication information cannot be ensured.

* Validity Period (s) s

* Algorithm ▼

Algorithm A is an insecure algorithm, please choose with caution.

Sign Algorithm ▼

The signature algorithm has been modified, requiring adaptation for generating authentication URLs. For details, refer to the [documentation](#).

Cancel
OK

Table 4-5 Parameters

Parameter	Description
Signing Key	<p>You can enter a key or click Generate on the right to automatically generate one.</p> <p>Note:</p> <ul style="list-style-type: none"> You are advised to use an auto-generated key. Keys that are not sufficiently random may compromise authentication security. The key cannot be queried after being set. Keep it secure. If the key is lost, reset it or submit a service ticket to request access.

Parameter	Description
Secondary Key	<p>You can enter a key or click Generate on the right to automatically generate one.</p> <p>Note:</p> <ul style="list-style-type: none"> You are advised to use an auto-generated key. Keys that are not sufficiently random may compromise authentication security. The key cannot be queried after being set. Keep it secure. If the key is lost, reset it or submit a service ticket to request access.
Validity Period	<p>How long a signed URL remains valid. The default value is 120 minutes.</p> <p>For example, if the signed URL is generated at 1573806090 (Nov. 15, 2019 16:21:30 GMT+08:00) with a validity period of 120 minutes, the URL expires at Nov. 15, 2019 18:21:30 GMT+08:00.</p>
Algorithm	<p>Key encryption algorithm. The following algorithms are supported:</p> <p>Algorithms A, B, and C: use the MD5 message-digest algorithm. For details, see Encryption Algorithm A, Encryption Algorithm B, and Encryption Algorithm C.</p> <p>Algorithm D: uses symmetric encryption. For details, see Encryption Algorithm D.</p> <p>Algorithm E: uses the SHA256 algorithm. For details, see Encryption Algorithm E (same as the Signing Method C2 of CDN).</p> <p>NOTE</p> <ul style="list-style-type: none"> Algorithms A, B, C, and D are insecure. Algorithm E is recommended. Algorithms A, B, and C do not support HLS or DASH playback. Algorithm E is recommended. If you modify the URL validation settings, such as changing the algorithm or key, you are advised to verify the settings before distribution.
Signature Algorithm	<p>Algorithms A, B, and C support SHA-256. MD5 is available for existing users by default.</p> <p>Note:</p> <ul style="list-style-type: none"> If you need to change the signature algorithm for key encryption algorithm A, B, or C, generate signed URLs by referring to Generating a Signed URL (Demo). Otherwise, playback will fail. MD5 is not recommended because it is insecure.

Parameter	Description
Authentication Scope	Defines which files require authentication. You can choose to authenticate all files, authenticate only files with specific extensions, or exclude files with specific extensions from authentication.
Authentication Inherit Config	<p>Adds authentication parameters to TS and MP4 files referenced by M3U8/MPD index files so they can be played after authentication succeeds.</p> <p>NOTE</p> <ul style="list-style-type: none"> For multi-layer M3U8/MPD files, only the first-layer M3U8/MPD files are parsed. TS/MP4 streams referenced by deeper layers are not expanded. Standard M3U8 is supported. Files are parsed line by line. If parsing fails, the origin server response is returned. URIs in #EXT-X-MAP and URLs/URIs on lines not starting with # are supported. Standard MPD is supported. Files are parsed line by line. If parsing fails, the origin server response is returned. URIs between tags <BaseURL> and </BaseURL> are identified. The SegmentTemplate tag is not supported.
Preview	<p>Only HLS and MP4 files can be previewed.</p> <p>NOTE</p> <p>Only algorithms D and E support preview, but they work exclusively with HLS and MP4 files. MP4 preview takes effect only when MOOV precedes MDAT. After preview is enabled, playback URLs can be obtained from the VOD console. The default preview duration is 300s.</p>

Step 5 Click **OK**.

Step 6 Verify whether the URL validation settings have taken effect.

Obtain a signed playback URL and play the content via the URL. If the playback is successful, the URL validation settings have taken effect.

----End

Generating a Signed URL

Obtaining a Signed URL on the Console

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

Step 2 In the navigation pane, choose **Management > Audio and Video Management**.

Step 3 Click **Details** in the row containing your media file and then choose the **Playback** tab.


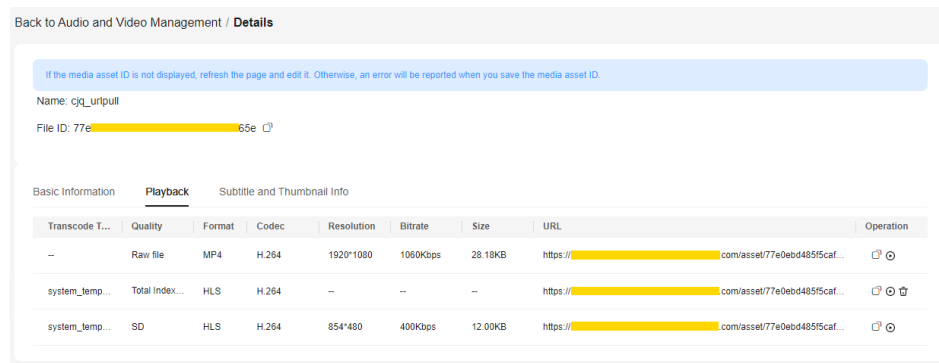
The **URL** column displays the original streaming URL of the media file. Click  to obtain the signed URL.

Figure 4-21 Playback URL



----End

Encryption Algorithm A

Signed URL format

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

Formula for calculating **auth_key**

auth_key = {MD5 or SHA256}(/asset/{assetId}/{file_name}-{timestamp}-{rand}-{uid}-{private_key})

Table 4-6 Authentication fields

Field	Description
timestamp	Time when a signed URL is generated. The value is a Unix timestamp, which is the number of seconds since January 1, 1970. Example: 1564731935 (2019.08.02 15:45)
rand	Random number. The recommended value is a UUID, which cannot contain hyphens (-). Example: f03cbe7c4a3849bc8d8769e3110e4533
uid	This parameter is not used now. Set it to 0 .
private_key	Key value set on the console. For details, see Procedure .

Signed URL example

Original URL: http://1.cdn.myhuaweicloud.com/asset/6b2d740f10b8697d8ea6672868ecdb6f/test.mp4
private_key: myPrivateKey
timestamp: 1547123166
rand: 477b3bbc253f467b8def6711128c7bec
uid: 0

Take MD5 as an example. Obtain **auth_key** according to the calculation formula.

auth_key = md5(/asset/6b2d740f10b8697d8ea6672868ecdb6f/
test.mp4-1547123166-477b3bbc253f467b8def6711128c7bec-0-myPrivateKey) =
584883719a3f722bf1a32a3b0a4d25dd

Signed URL with algorithm A

http://1.cdn.myhuaweicloud.com/asset/6b2d740f10b8697d8ea6672868ecdb6f/test.mp4?
auth_key=1547123166-477b3bbc253f467b8def6711128c7bec-0-584883719a3f722bf1a32a3b0a4d25dd

Encryption Algorithm B

Signed URL format

`https://{cdn_domain}/{date_YYYYmmddHHMM}/{authStr}/asset/{asset_id}/{file_name}`

Formula for calculating **authStr**

`authStr = {MD5 or SHA256}({private_key}{date_yyyyMMddHHmm}/asset/{asset_id}/{file_name})`

Table 4-7 Authentication fields

Field	Description
date_yyyyMMddHHmm	Time when a signed URL is generated. The format is yyyyMMddHHmm. Example: 201908051445
file_name	Part starting behind the media asset ID of the original streaming URL to the end of the URL. Example: play_video/test.mp4
private_key	Key value set on the console. For details, see Procedure .

Signed URL example

Original URL: `http://1.cdn.myhuaweicloud.com/asset/6b2d740f10b8697d8ea6672868ecdb6f/test.mp4`
 private_key: myPrivateKey
 date_yyyyMMddHHmm: 201901102026
 file_name: test.mp4

Take MD5 as an example. Obtain **authStr** according to the calculation formula.

`authStr = md5(myPrivateKey201901102026/asset/6b2d740f10b8697d8ea6672868ecdb6f/test.mp4) = 713ef643de8df076da6ec3c0545968cb`

Signed URL with algorithm B

`http://1.cdn.myhuaweicloud.com/201901102026/713ef643de8df076da6ec3c0545968cb/asset/6b2d740f10b8697d8ea6672868ecdb6f/test.mp4`

Encryption Algorithm C

Signed URL format

`https://{cdn_domain}/{authStr}/{time_hex}/asset/{asset_id}/{file_name}`

Formula for calculating **authStr**

`authStr = {MD5 or SHA256}({private_key}/asset/{asset_id}/{file_name}{time_hex})`

Table 4-8 Authentication fields

Field	Description
file_name	Part starting behind the media asset ID of the original streaming URL to the end of the URL. Example: play_video/test.mp4

Field	Description
time_hex	Time when a signed URL is generated. The value is a hexadecimal Unix timestamp. Example: hex(1564987530)=5D47D08A
private_key	Key value set on the console. For details, see Procedure .

Signed URL example

Original URL: http://1.cdn.myhuaweicloud.com/asset/6b2d740f10b8697d8ea6672868ecdb6f/test.mp4
private_key: myPrivateKey
time_hex: hex(timestamp) = hex(1547123166) = 5C3739DE
file_name: test.mp4

Take MD5 as an example. Obtain **authStr** according to the calculation formula.
authStr=md5(myPrivateKey/asset/6b2d740f10b8697d8ea6672868ecdb6f/test.mp45C3739DE) =
afa20c956043fe6d130b16f2704ac870

Signed URL with algorithm C

http://1.cdn.myhuaweicloud.com/afa20c956043fe6d130b16f2704ac870/5C3739DE/asset/
6b2d740f10b8697d8ea6672868ecdb6f/test.mp4

Encryption Algorithm D

Signed URL format

Original URL?auth_info={Encrypted string}.{EncodedIV} &exper={exper}&plive={plive_starttime}

Formulas for calculating *Encrypted string* and **EncodedIV**:

- Original string:
 - **With preview enabled:** Original string = url_encoding({path})+"\$"+{Timestamp}+"\$"+{exper}
 - **With pseudo-streaming enabled:** Original string = url_encoding({path})+"\$"+{Timestamp}+"\$"+{plive_starttime}
- Encrypted string = aes_cbc_128_pkcs5padding(Original encrypted string,key,IV)
- EncodedIV = hex(IV)

Table 4-9 Authentication fields

Field	Description
path	Directory from the domain name to the last level, including the slash (/) behind the domain name and slash (/) behind the last level of directory, excluding the file name Example: /asset/32237c8f68fcc6071a2d8e3421eee20d/play_video/

Field	Description
Timestamp	Time when a signed URL is generated. The value is UTC time in yyyyMMddHHmmss format. Example: 20190805101025
key	Key value set on the console. For details, see Procedure .
(Optional) exper	Video preview duration, in seconds. Only MP4 and HLS videos can be previewed. For HLS, the master index cannot be previewed, but secondary indexes can. Specify this parameter only for preview. In other cases, this parameter is not required for calculating the signed URL.
(Optional) plive	Start time of pseudo-streaming, in UTC time. Specify this parameter only for pseudo-streaming. In other cases, this parameter is not required for calculating the signed URL. The preview and Pseudo-Streaming functions cannot be enabled at the same time.
IV	Randomly generated byte array. It can be up to 16 characters long. hex(): converts the byte array into a hexadecimal string. Sample code for generating IV is: <pre>byte[] iv = new byte[16]; SecureRandom secureRand = new SecureRandom(); secureRand.nextBytes(iv);</pre>

Signed URL example

Original URL: https://179.cdn-vod.huaweicloud.com/asset/32237c8f68fcc6071a2d8e3421eee20d/play_video/index.m3u8
 path: /asset/32237c8f68fcc6071a2d8e3421eee20d/play_video/
 key: 8Ks1qn14XRO28qOa
 Timestamp: 20190805102430
 exper: 300
 plive: 1704074400

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

- With preview enabled**
 Original string = url_encoding("/asset/32237c8f68fcc6071a2d8e3421eee20d/play_video/") + "\$" + "20190805102430" + "\$" + "300"
 Encrypted string = aes_cbc_128_pkcs5padding(Original string,key,IV) = 34M%2F6KtYgxuAozdBLIVTe0dUVAZdvXsYQoYAnDmuhRHH1hshYg%2B2TI0AmSwySDh%2BmKER44qYKpSP%2BgfsLM%2FIZe4F6K4n1Nx6ouGwyKfqdDA%3D
 EncodedIV = hex(IV) = 79436d453636364e335941713330534e
- With pseudo-streaming enabled**
 Original string = url_encoding("/asset/32237c8f68fcc6071a2d8e3421eee20d/play_video/") + "\$" + "20190805102430" + "\$" + "1704074400"
 Encrypted string = aes_cbc_128_pkcs5padding(Original string,key,IV) = 34M%2F6KtYgxuAozdBLIVTe0dUVAZdvXsYQoYAnDmuhRHH1hshYg%2B2TI0AmSwySDh%2BmKER44qYKpSP

```
%2BgfsLM%2FZe4F6K4n1Nx6ouGwyKfqdDA%3D
EncodedIV = hex(IV) = 79436d453636364e335941713330534e
```

Signed URL with algorithm D

- With preview enabled
`https://179.cdn-vod.huaweicloud.com/asset/32237c8f68fcc6071a2d8e3421eee20d/play_video/index.m3u8?auth_info=34M%2F6KtYgxuAozdBLIVTe0dUVAZdvXsYQoYAnDmuhRHH1hshYg%2B2Tl0AmSwySDh%2BmkER44qYKpSP%2BgfsLM%2FZe4F6K4n1Nx6ouGwyKfqdDA%3D.79436d453636364e335941713330534e&exper=300`
- With pseudo-streaming enabled
`https://179.cdn-vod.huaweicloud.com/asset/32237c8f68fcc6071a2d8e3421eee20d/play_video/index.m3u8?auth_info=34M%2F6KtYgxuAozdBLIVTe0dUVAZdvXsYQoYAnDmuhRHH1hshYg%2B2Tl0AmSwySDh%2BmkER44qYKpSP%2BgfsLM%2FZe4F6K4n1Nx6ouGwyKfqdDA%3D.79436d453636364e335941713330534e&plive=1704074400`

Encryption Algorithm E



The preview and pseudo-streaming functions cannot be enabled at the same time. The following URLs are for reference only. **exper** and **plive** cannot exist at the same time.

Signed URL format

```
Original URL?auth_key={authKey}&timestamp={timestamp}&exper={exper}&plive={plive_starttime}
```

Formula for calculating **authKey**:

- With preview enabled: $auth_key = sha256(\{PrivateKey\}\{fileName\}\{timestamp\}\{exper\})$
- With pseudo-streaming enabled: $auth_key = sha256(\{PrivateKey\}\{fileName\}\{timestamp\}\{plive_starttime\})$

Table 4-10 Authentication fields

Field	Description
timestamp	Time when a signed URL is generated. The value is a Unix timestamp, which is the number of seconds since January 1, 1970. Unit: second. Example: 1564731935, that is, the time is 2019.08.02 15:45.
fileName	Back-to-origin URL. During authentication, the value must start with a slash (/) and cannot include the parameters behind ? in the signed URL. Example: /asset/6b2d740f10b8697d8ea6672868ecdb6f/test.hls

Field	Description
PrivateKey	Signing key, which is used to generate a signed URL. The key can contain 16 to 32 characters. Only letters and digits are allowed.
(Optional) exper	Video preview duration, in seconds. Only MP4 and HLS videos can be previewed. For HLS, the master index cannot be previewed, but secondary indexes can. Specify this parameter only for preview. In other cases, this parameter is not required for calculating the signed URL.
(Optional) plive	Start time of pseudo-streaming, in UTC time. This field is valid only for the HLS format. Specify this parameter only for pseudo-streaming. In other cases, this parameter is not required for calculating the signed URL. The preview and Pseudo-Streaming functions cannot be enabled at the same time.

Signed URL example

Original URL: `http://1.cdn.myhuaweicloud.com/asset/6b2d740f10b8697d8ea6672868ecdb6f/test.hls`
 private_key: `32d6b2d740f10b86`
 timestamp: `1547123166`
 fileName: `/asset/6b2d740f10b8697d8ea6672868ecdb6f/test.hls`
 exper: `300`
 plive: `1704074400`

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

- Preview enabled

`auth_key = sha256(32d6b2d740f10b86/asset/6b2d740f10b8697d8ea6672868ecdb6f/test.hls1547123166300) = 3a935cf1d8299fe63ec8d4e0afb5ef3304883a702a4e760f3c5ae838a4b69768`

- Pseudo-streaming enabled

`auth_key = sha256(32d6b2d740f10b86/asset/6b2d740f10b8697d8ea6672868ecdb6f/test.hls15471231661704074400) = 3a935cf1d8299fe63ec8d4e0afb5ef3304883a702a4e760f3c5ae838a4b69768`

Signed URL with algorithm E

- Preview enabled

`http://1.cdn.myhuaweicloud.com/asset/6b2d740f10b8697d8ea6672868ecdb6f/test.hls?auth_key=3a935cf1d8299fe63ec8d4e0afb5ef3304883a702a4e760f3c5ae838a4b69768×tamp=1547123166&exper=300`

- Pseudo-streaming enabled

`http://1.cdn.myhuaweicloud.com/asset/6b2d740f10b8697d8ea6672868ecdb6f/test.hls?auth_key=3a935cf1d8299fe63ec8d4e0afb5ef3304883a702a4e760f3c5ae838a4b69768×tamp=1547123166&plive=1704074400`

4.6 Pseudo-Streaming

Pseudo-streaming leverages the playback control capability of VOD to play VOD files like a livestream. You can generate VOD files, specify the time of starting a

livestream, and use VOD to distribute streaming-like content, reducing livestream risks and costs. Pseudo-streaming does not support fast forward and is ideal for online teaching videos, gala livestreaming, and broadcasting and television.

Highlights

Highlights of pseudo-streaming:

- **Easy operation:** Pseudo-streaming does not require livestreaming rooms. Any video can generate a pseudo livestream at any time. Pseudo-streaming can be implemented simply by enabling the transcoding and hotlink protection functions of VOD.
- **Enhanced livestream security:** Pseudo-streaming allows reviewing and editing VOD files in advance, such as deleting inappropriate content, to keep the livestream secure.

Application Scenarios

Pseudo-streaming is mainly used for pre-recorded videos. A pseudo livestream starts at the specified time for users to watch. Users can obtain the link to the pseudo livestream in advance, but can watch the video only after the specified time.

Application scenarios:

- **Online education:** The validity period of the streaming URL is set for a recorded video to remind trainees to watch the video on time. If the streaming URL expires, trainees need to obtain another streaming URL to watch the video.
- **Entertainment:** Pre-recorded TV programs, such as variety shows, can be favorited by the target audience in advance and watched on time.
- **Activities:** The activity organizer pre-records the activity video and releases a bulletin with the streaming URL. Users can save the streaming URL in advance and access it when the activity starts.

Notes

Pseudo-streaming is still a feature of VOD. Here are some precautions of using pseudo-streaming:

- The source video quality is fundamental.
- Pseudo-streaming is applicable only to HLS videos, with segment duration of 2 to 4 seconds, even segment distribution, and bitrate lower than 5 Mbit/s.
- HLS files transcoded on Huawei Cloud VOD are recommended.
- Pseudo-streaming is a livestreaming-like service and does not allow pausing or stopping video playback, or modifying video content such as real-time transcoding and watermarking.
- Currently, audio of a video cannot be separated from the video.

Procedure

Step 1 Log in to the [VOD console](#).

Step 2 In the navigation pane, choose **Audio and Video Uploads > Local Upload** to upload an audio/video file from the local PC.

For details, see [Audio/Video Upload](#).

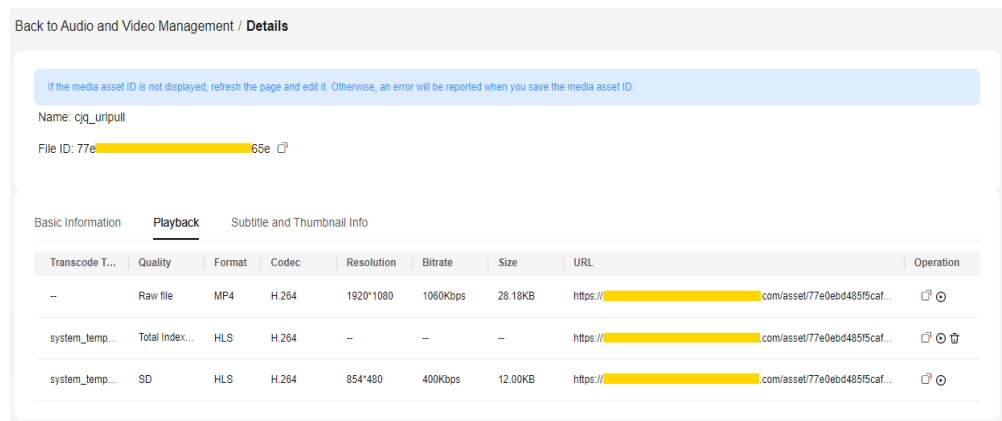
Step 3 Pseudo-streaming is applicable only to HLS videos, so you need to convert the video to an HLS one if it is not.

1. In the navigation pane, choose **Management > Audio and Video Management**.
2. Select the uploaded video and click **Transcode** to convert the video to an HLS one.

For details, see [Transcoding](#).

3. Click **Details** on the right of the video file and view the HLS streaming URL under the **Playback** tab, as shown in [Figure 4-22](#).

Figure 4-22 Streaming URL



Step 4 Enable URL validation before using pseudo-streaming.

1. In the navigation pane, choose **Domain Name Management**.
2. Click **Configure** on the right of the domain name and choose the **Hotlink Protection Settings** tab.
3. Click **URL Validation** and toggle on the **Status** switch.
4. Configure URL validation parameters by referring to [URL Validation](#).

The pseudo-streaming switch is displayed only when **Algorithm** is set to **Algorithm D** or **Algorithm E**. The pseudo-streaming switch must be toggled on, and pseudo-streaming is applicable only to HLS videos.

5. Calculate the signed URL for algorithm D or E by referring to [Encryption Algorithm D](#) or [Encryption Algorithm E](#).

After pseudo-streaming is enabled, the parameter **plive** is added to the encryption algorithm. **plive={plive_starttime}** is added to the streaming URL to calculate the encrypted string.

Example: `https://example.com/index.m3u8?`

`auth_key={authKey}×tamp={timestamp}&plive=1704074400`

plive_starttime indicates when the pseudo-streaming starts (in UTC time). For example, **1704074400** indicates that the pseudo-streaming starts at 10:00 on January 1, 2024.

- Step 5** You can use pseudo-streaming by accessing the signed URL on an HLS-compatible player.

NOTICE

The Chrome browser does not support HLS by default. You need to install a plug-in.

----End

5 Audio/Video Upload

5.1 Overview

After enabling VOD, you can upload audio/video files to VOD for management.

- **Local upload:** uploads audio/video files stored on local disks to VOD
- **Pull from URLs:** pulls source audio/video files from their URLs and then upload them to VOD

Constraints

Supported audio/video file formats:

- Video: MP4, TS, MOV, MXF, FLV, MPG, WMV, AVI, M4V, F4V, MPEG, 3GP, ASF, MKV, WEBM, RMVB, VOB, RM, MTS, DV, DAT, QT, M2T, SWF and M3U8. M3U8 files can be uploaded only by URL pull.
- Audio: MP3, OGG, WAV, WMA, APE, FLAC, AAC, AC3, MMF, AMR, M4A, M4R, WV, MP2, RA, and CAF

Any spaces in filenames will be deleted once the files are uploaded.

HLS media files can be ingested and played, but processing operations (such as screenshot capturing, parsing, transcoding, and review) on HLS source files are not supported.

Prerequisites

- To categorize media files, create categories by referring to [Category Settings](#).
- To keep yourself informed of the upload progress, configure event notifications by referring to [Overview](#).
- To transcode these files, create a transcoding template by referring to [Transcoding Settings](#).
- To process these files using a workflow, create a workflow by referring to [Workflow Settings](#).

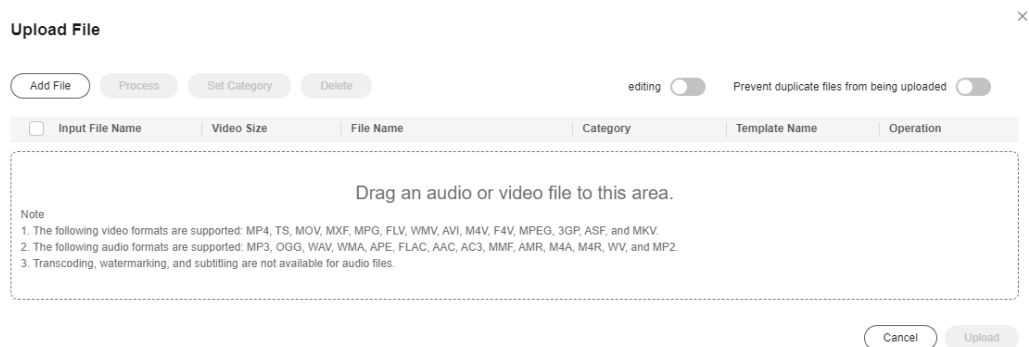
5.2 Local Upload

Audio/Video files stored on local disks can be uploaded to VOD.

Procedure

- Step 1** Log in to the [VOD console](#).
- Step 2** In the navigation pane, choose **Audio and Video Uploads > Local Upload**.
- Step 3** Click **Upload File**. The **Upload File** dialog box is displayed.
- Step 4** Click **Add File** to add a local media file, or directly drag a file to the file area, as shown in [Figure 5-1](#).

Figure 5-1 Local upload



- Step 5** Toggle on the **Prevent duplicate files from being uploaded** switch to avoid waste of time and storage space.

Configure this parameter as required. If you add a duplicate media file, an error message is displayed in the upper right corner.

- Step 6** Categorize uploaded files, change the file names, or process these files.

If audio/video processing is not required, retain the default settings. If audio/video processing is required, click **Process** and configure the parameters by referring to [Table 5-1](#).

Figure 5-2 Processing media files

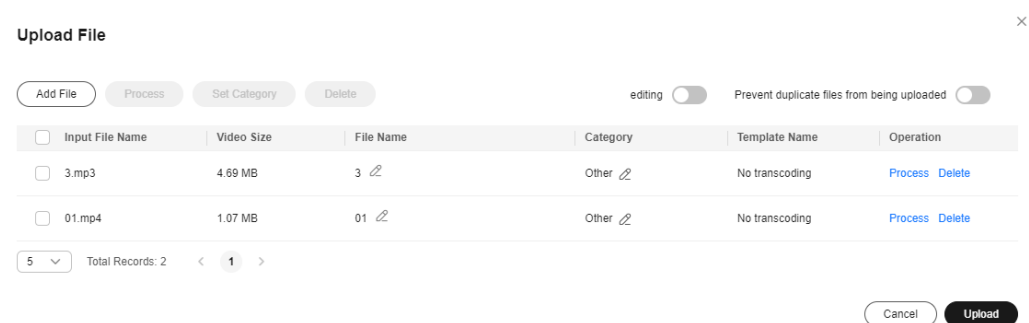


Table 5-1 Parameters

Parameter	Description
Transcoding template group	Select a preset template group or customize a template group by referring to Transcoding Settings .
Workflow	Select an existing workflow or create one by referring to Workflow Settings .

Step 7 Click **Upload**.

Note:

- The upload duration depends on the file size and network conditions. During the upload, do not refresh the page, clear the browser cache, or close the browser.
- If there is no activity for an extended period during the upload, you may be logged out and the upload will fail.

Step 8 View media file information on the [Audio and Video Management](#) page.

After a video file is uploaded, the first frame at the first second is used as the thumbnail by default. If a transcoding template group or workflow was configured during media file upload, the configured parameters will automatically apply to the media file processing.

----End

5.3 Pull from URLs (OBT)

Audio/Video files can be pulled from their URLs and uploaded to VOD.

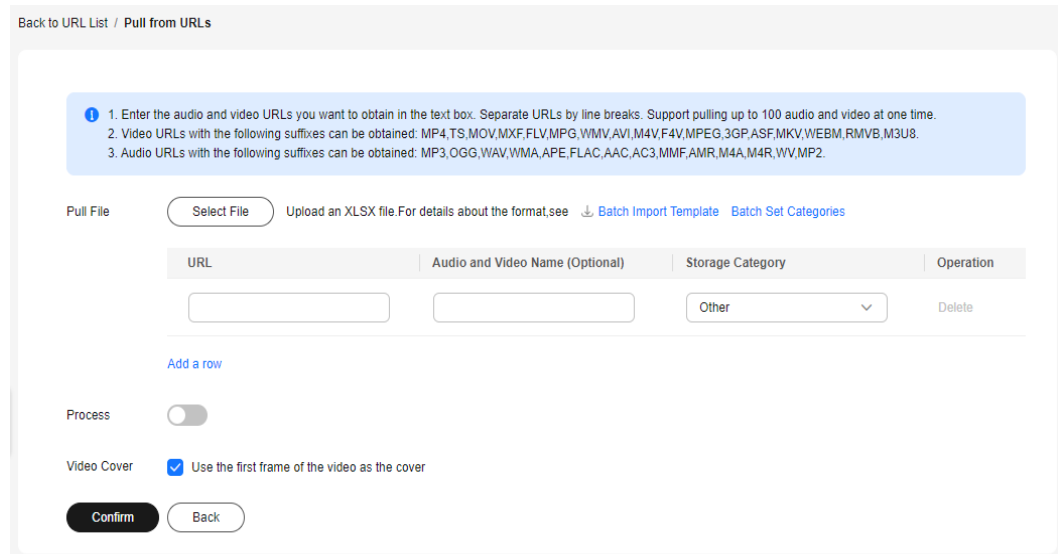
Procedure

Step 1 Log in to the [VOD console](#).

Step 2 In the navigation pane, choose **Audio and Video Uploads > Pull from URLs**.

Step 3 Click **Pull from URLs**. The **Pull from URLs** page is displayed, as shown in [Figure 5-3](#).

Figure 5-3 Settings of pull from URLs



See [Table 5-2](#).

Table 5-2 Parameters

Parameter	Description
Pull File	<p>Constraints:</p> <ul style="list-style-type: none"> • A URL must contain the filename extension, for example, https://xxx.mp4. • Files can be pulled from a maximum of 100 URLs. • Currently, only HTTPS (recommended) and HTTP (risky) are supported. <p>You can add the file(s) to be pulled in either of the following ways:</p> <ul style="list-style-type: none"> • Adding one file: Enter information about the audio/video file to be pulled in the audio/video file URL and audio/video file name columns. • Batch adding files: Click Batch Import Template to download the template file to the local PC. After all audio/video file URLs and names are added, click Select File to import files. <p>NOTE Do not attach sensitive information such as authentication credentials to the URLs that pull content.</p>
Process	<p>Determine whether to process the obtained audio/video files. This function is disabled by default. To enable it, you need to select the processing mode, that is, to select a transcoding template group or a workflow.</p>

Parameter	Description
Select Process Mode	<p>This parameter is displayed only when Process is enabled. Click Select on the right of Select Process Mode. On the dialog box displayed, configure the following parameters:</p> <ul style="list-style-type: none"> ● Transcoding template group: Select a preset template group or customize a template group by referring to Creating a Template Group. ● Workflow: Select an existing workflow or create one by referring to Workflow Settings.
Video Cover	Sets whether to use the first frame of the video as the thumbnail.

Step 4 Click **Confirm**. You can view the task status in the URL pull list.

When the status becomes **Completed**, the pull is successful. You can view audio/video information on the [Audio and Video Management](#) page.

Figure 5-4 URL pull status

Pull from URLs (OBT)

Buttons: Pull from URLs, Cancel, retry, Delete. Filter: All

URL	Name	ID	Status	Created	Operation
<input type="checkbox"/> https://103-cn-north-4.cd...	41fe963003b8bbd409...	a3d150e48231f388ab...	Completed	2024/8/27 11:48:32	Delete
<input type="checkbox"/> https://video.coolcollege....	47f5b7b-188b7cb04fa...	b2f0c3b4543897ce06...	Completed	2024/8/23 16:43:30	Delete
<input type="checkbox"/> https://103-cn-north-4.cd...	606a341db520d9b505...	adfd232178a5f081a23...	Completed	2024/8/23 16:43:30	Delete
<input type="checkbox"/> https://video.coolcollege....	47f5b7b-188b7cb04fa...	65d4a9f4299ca051ee...	Completed	2024/8/6 14:14:02	Delete
<input type="checkbox"/> https://103-cn-north-4.cd...	606a341db520d9b505...	fe77b02d4661746a90...	Completed	2024/8/2 11:23:36	Delete
<input type="checkbox"/> https://103-cn-north-4.cd...	606a341db520d9b505...	849cecabd1423ab58b...	Completed	2024/8/2 11:23:36	Delete
<input type="checkbox"/> https://103-cn-north-4.cd...	606a341db520d9b505...	aabe90f92f62156a428...	Completed	2024/8/2 11:23:36	Delete
<input type="checkbox"/> https://103-cn-north-4.cd...	606a341db520d9b505...	0a39d557cbfe7251a2...	Completed	2024/8/2 11:23:36	Delete
<input type="checkbox"/> https://103-cn-north-4.cd...	606a341db520d9b505...	bf090e909fcc7407355...	Completed	2024/8/2 11:23:36	Delete
<input type="checkbox"/> https://103-cn-north-4.cd...	606a341db520d9b505...	042ee576dddca47363...	Completed	2024/8/2 11:23:36	Delete

Total Records: 1,206 | 10 | < 1 2 3 4 5 6 ... 121 >

----End

6 Media Asset Management

6.1 Audio/Video Management

After **uploading audio/video files**, you can use functions such as transcoding, categorization, CDN pre-loading, CDN refresh, storage class change, audio extraction, and one-click information export on the **Audio and Video Management** page.

The management functions vary depending on audio and video files. See **Table 6-1**.

Table 6-1 Management functions

Function	Video (√: Supported; ×: Not Supported)	Audio (√: Supported; ×: Not Supported)
Uploading a Thumbnail	√	√
Subtitling	√	√
Transcoding and Transcoding Cancellation	√	×
Pre-loading	√	√
CDN Cache Refreshing	√	√
Categorization	√	√
Storage Class Change	√	√
Restoring an Archived File	√	√
Audio Extraction	√	×
Publishing	√	√
Exporting	√	√

Function	Video (√: Supported; ×: Not Supported)	Audio (√: Supported; ×: Not Supported)
Searching for Audio/Video Files	√	√
Playback	√	√
Deleting Audio/Video Files	√	√

Viewing Media Asset Information

You can click **Details** on the right of the audio/video file to view the following information:

- Basic Information**
 Media asset name, ID, thumbnail, subtitle, duration, size, upload time, last update time, category, tag, and description.
- Playback**
 Definitions, formats, video encoding formats, resolution levels, bitrates, sizes, and streaming URLs of the source file and transcoded file.
- Subtitle and Thumbnail Info**
 If you have added subtitles and a thumbnail for the uploaded file, you can view the format and address of the subtitles and thumbnail on this page.

Modifying Basic Information

Under the **Basic Information** tab, you can change the category, label, name, and description of the audio/video file.

- Step 1** Click **Details** on the right of the audio/video file. Under the **Basic Information** tab, click **Edit**.
- Step 2** Click **Set Category** to reset the category of the media asset.
- Step 3** Specify **Category**, **Name**, and **Description** so that you can use advanced search to search for media files.
- Step 4** Click **Save**. The updated description and category are displayed.

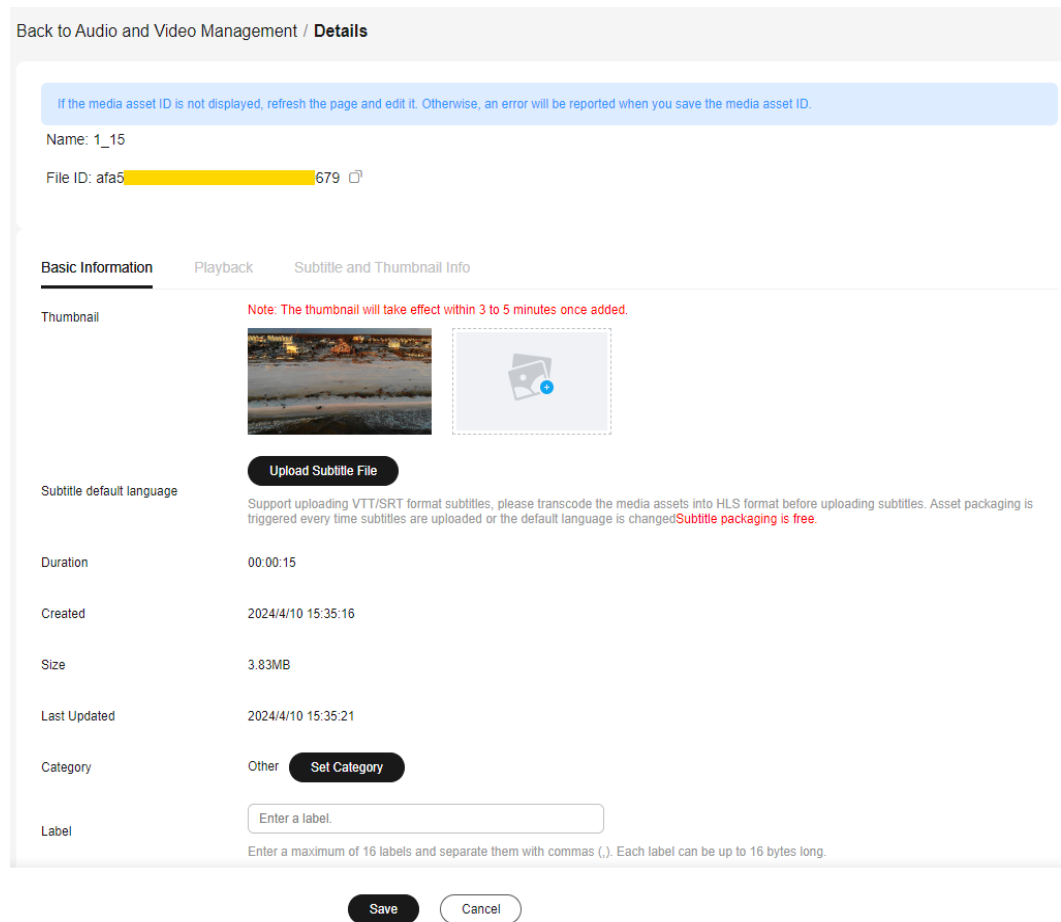
----End

Uploading a Thumbnail

After an audio/video file is uploaded, the first frame is captured as the thumbnail by default. You can also upload a JPG or PNG image as the thumbnail. Before using a video frame as the thumbnail, use **snapshot capturing** to capture a video frame.

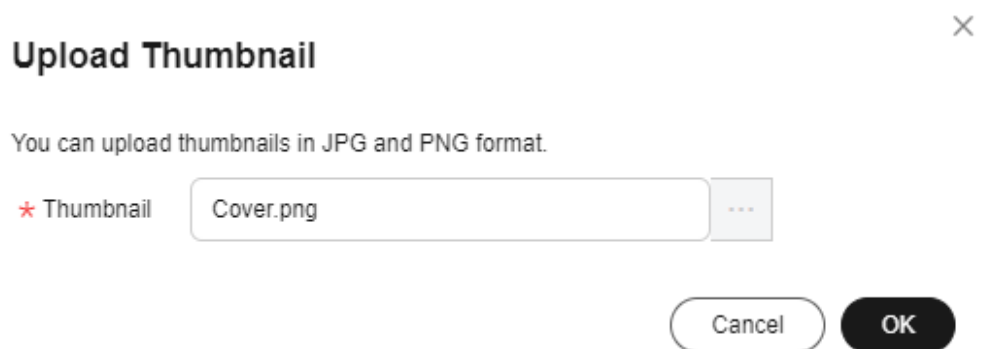
- Step 1** Click **Details** on the right of the audio/video file. Under the **Basic Information** tab, click **Edit**.

Figure 6-1 Media asset details



Step 2 Click the plus sign next to **Thumbnail**. In the **Upload Thumbnail** dialog box, select a local image file.

Figure 6-2 Uploading a thumbnail



Step 3 Click **OK**. The modification will take effect in 3 to 5 minutes.

----End

Subtitling

NOTICE

- External subtitles are not supported for HLS outputs that are saved to a different OBS bucket but in the same directory as input files.
- If the language you specify is not in the subtitle list in the HLS index file, the configuration will fail.
- Subtitling is not supported if you use the **original_template_group**.
- External subtitles are not supported when both HLS and DASH outputs are generated using a template group. For details about how to create a transcoding template group, see [Creating a Transcoding Template Group](#).
- The native iOS browser Safari does not support parsing and playing of VTT subtitle files.

VOD supports subtitle files in VTT and SRT formats. You can upload multiple subtitle files. By default, one language maps to one subtitle file.

VOD supports the following two types of subtitles:

- Embedded subtitles
 - Subtitle files are integrated into video files, so there are no longer separate subtitle files.
 - For single-file videos (such as MP4 and MOV), you can upload SRT subtitle files encoded in UTF-8.
 - Only non-HLS videos or large videos generated after transcoding support embedded subtitles.
 - Only one subtitle file is supported.
 - To generate embedded subtitles, you must upload subtitle files and then transcode videos to produce versions with embedded subtitles. If you add a subtitle file after transcoding, you must transcode the video again to generate a new version with embedded subtitles.
 - When generating a video with embedded subtitles, the subtitle file in the default language is used first. By default, the most recently uploaded SRT subtitle file is used.
 - Deleting subtitle files does not affect videos that have already been generated with embedded subtitles. However, newly generated videos will contain no subtitles.
- External subtitles
 - Subtitles remain as separate files and are applied externally.
 - For HLS videos generated after transcoding, you can upload SRT or VTT subtitle files. No re-transcoding is required to enable external subtitles.
 - Only HLS videos generated after transcoding support external subtitles.
 - Multiple external subtitles are supported. That is, you can add multiple subtitle files, with one file corresponding to a language. The player will include options for the default language and all other available subtitle languages, allowing users to select their preferred subtitle language during playback.

- You can set a default language for external subtitles. For HLS videos, changes to the default language take effect immediately.
- Deleting subtitle files does not affect transcoded videos that already have external subtitles. It only affects newly generated videos, that is, they will have no subtitles.

The procedure is as follows:

Step 1 Click **Details** on the right of the audio/video file. Under the **Basic Information** tab, click **Edit**.

Step 2 Click **Upload Subtitle File** to open the **Upload Subtitle File** dialog box, as shown in **Figure 6-3**.

Configure the parameters by referring to **Table 6-2**.

Figure 6-3 Uploading a subtitle file

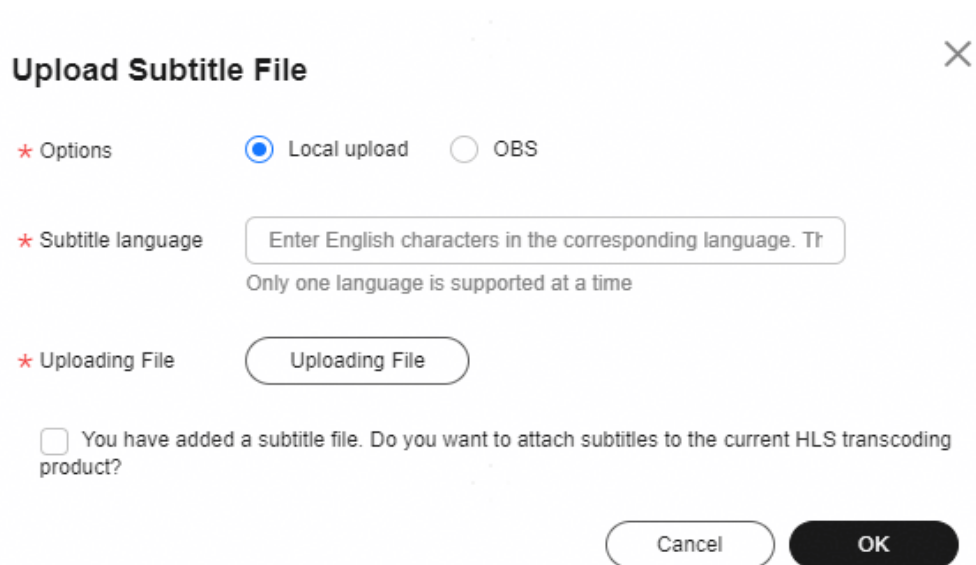


Table 6-2 Uploading a subtitle file

Parameter	Description
Options	Select the subtitle upload mode. Options: <ul style="list-style-type: none"> • Local upload • OBS
Subtitle Language	Enter the English code for the corresponding language. Only one language is supported at a time.
Local upload	Click Upload File and select a local subtitle file.
OBS upload	Enter the OBS bucket name and path of the subtitle file.

Step 3 Click **OK**. The subtitle file is uploaded.

You can click **Set as Default Language** on the right of the subtitle file to make the current subtitle file the default.

Step 4 Add subtitles in multiple languages by repeating **Step 2** to **Step 3**.

This operation is required only for adding external subtitles.

Step 5 Click **Save**.

Step 6 Generate a video with embedded subtitles or external subtitles.

1. Return to the **Management > Audio and Video Management** page, select the video, and click **Transcode** to generate a video with embedded subtitles or external subtitles.
2. Click **Details** on the right of the audio/video file. The subtitle file URL is displayed under the **Subtitle and Thumbnail Info** tab.

----End

Transcoding

CAUTION

If the source file is transcoded successfully but the output video is shorter than the original, this is related to the current transcoding mechanism.

- If the source contains a short abnormal segment, that segment is dropped. For example, if in a 10-minute video, the content becomes abnormal after minute 9, the transcoded video will be 9 minutes long, with the abnormal final minute removed.
- If the source contains a long abnormal segment, for example, more than 3 minutes, transcoding will fail.

On the **Audio and Video Management** page, you can select one or more audio/video files for transcoding.

- Supported input audio formats: MP4, TS, MOV, FLV, MPG, MXF, WMV, ADTS, AVI, MKV, MPEG, VOB, RM, and MTS
- Supported input video codecs: H.264, H.265, MPEG-2, MPEG-4, MJPEG, WMV1/2/3, and ProRes 422
- Supported input audio codecs: AAC, AC3, EAC3, HE-AAC, MP2, MP3, PCM (s16le, s16be, s24le, s24be, DVD), and WMA

Step 1 Select one or more audio/video files and click **Transcode**.

Step 2 In the dialog box displayed, select a preset template or a custom template configured in **Transcoding Settings**, and click **OK**.

Step 3 View the status of the audio/video file on the **Audio and Video Management** page. The status becomes **Running**.

Step 4 After the transcoding is complete, click **Details** on the right of the audio/video file to obtain the streaming URL under the **Playback** tab.

----End

Pre-loading

Pre-loading allows you to proactively push videos to CDN PoPs. When users access a video for the first time, CDN can serve it from cache, reducing the pressure on the origin server.

Step 1 Select one or more audio/video files.

Step 2 Click **Pre-load**.

The time required to complete a pre-loading task depends on the number and size of files to be pre-loaded, and on network conditions.

----End

CDN Cache Refreshing

CDN cache refreshing is the opposite of **Pre-loading**. It forces the resources cached on CDN PoPs to expire. When a user next requests a resource, CDN pulls the latest version from the origin server, returns it to the user, and caches it on CDN PoPs.

Step 1 Select one or more audio/video files.

Step 2 Click **CDN Refresh** to forcibly expire the resources cached on CDN PoPs.

The time when the CDN refresh is complete depends on the number and size of files submitted, network conditions, and other factors.

----End

Categorization

Select one or more audio/video files and click **More Actions** > **Set Category** to categorize the selected audio/video files.

Changing the Storage Class

You can change the storage class of audio/video files in OBS on the **Management** > **Audio and Video Management** page. For details, see **OBS Storage Classes**.

The storage class of an uploaded audio/video file is Standard by default, and can be changed to Infrequent Access or Archive.

- Infrequent Access can be changed to Standard or downgraded to Archive.
- Archive can only be changed to Standard and cannot be directly changed to Infrequent Access.
- The storage class cannot be changed when a media asset has an ongoing task, such as snapshot capturing or transcoding.

The operations for changing the storage class of an audio/video are the same for all storage classes. The following describes how to change the storage class from Standard to Infrequent Access.

- Step 1** Select one or more audio/video files and choose **Modify the storage type > infrequently accessed storage**.
- Step 2** In the displayed dialog box, click **Confirm**.
- Step 3** Refresh the **Audio and Video Management** page. The storage class of the audio/video files has been changed to Infrequent Access.

----End

Restoring an Archived File

- Step 1** Select one or more audio/video files of the Archive storage class and click **Restore archived files**.

The **Restore archived files** dialog box is displayed.

Figure 6-4 Restoring archived files

Restore archived files ✕

After the asset is restored, a copy of the standard storage type object is generated. The copy has a validity period. After the validity period expires, the copy will be automatically deleted.

Revertive mode ▼
The restoration takes about 6 minutes.

Recovery mode Temporarily Retrieve Forever

* Copy Validity Period day(s)
Retention period of a restored object. The value ranges from 1 to 30.

See [Table 6-3](#).

Table 6-3 Parameters

Parameter	Description
Restoration mode	The time it takes an audio/video file to change the storage class from Archive to Standard. Options: <ul style="list-style-type: none">• Quick retrieval mode: The change takes about six minutes.• Standard retrieval mode: The change takes about three to five hours.
Recovery mode	Mode of restoring an audio/video file to the Standard storage class. Options: <ul style="list-style-type: none">• Temporarily: After an audio/video file is temporarily retrieved, a copy of the object in the Standard storage class is generated. In this case, you can access the audio/video file stored in OBS, but the temporarily restored file cannot be transcoded. The copy has a validity period and will be automatically deleted after the validity period ends. The actual storage class of the audio/video file is Archive.• Forever: An audio/video file is permanently retrieved and its storage class becomes Standard.
Copy Validity Period	Retention duration of the Standard object copy generated from the Archive audio/video file that is temporarily retrieved. Unit: day. Value range: 1 to 30.

Step 2 Click **Confirm**. The archived file has been restored.

When the retrieval time arrives, refresh the **Audio and Video Management** page.

- For temporary retrieval, the storage class of the audio/video is Archive.
- For permanent retrieval, the storage class of the audio/video is Standard.

----End

Audio Extraction

If you need the audio content of a video file, you can extract audio from the video file and then save the extracted audio file in MP3 format.

Step 1 Select one or more video files and click **More Actions > Extract Audio**.

Step 2 Refresh the audio/video management page. The status of the audio extraction task becomes **Running**.

Step 3 View the extracted audio file when **Transcoding Status** becomes **Completed**.

The extracted audio file and the source video file should have the same name. You can also check the audio file from its description.

----End

Publishing

Select one or more audio/video files and choose **More Actions > Publish** to publish the files. The files are in the **Published** status.

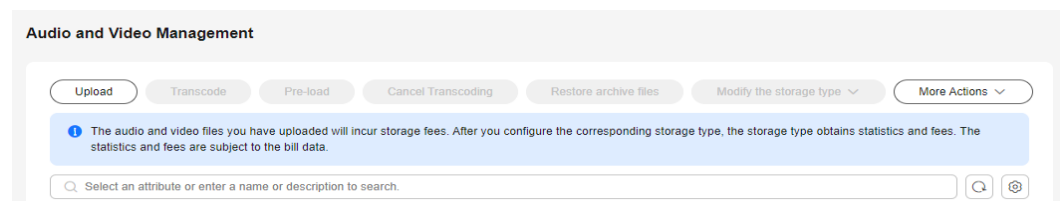
Exporting Media Asset Information

Select one or more audio/video files and choose **More Actions > Export** to export information about the selected files. If you do not select any file, information about all audio/video files is exported by default. The exported information about a media asset includes the ID, name, status, tag, category, resolution, streaming URL, thumbnail, and subtitle URL.

Searching for Audio/Video Files

If there are a large number of files on the **Audio and Video Management** page, you can use the filter criteria box in the upper part of the page to search for audio/video files, as shown in [Figure 6-5](#).

Figure 6-5 Searching for audio/video files



You can search for audio/video files by filter criteria (upload time, media asset status, transcoding status, name or description, media asset ID, tag, and category ID).

Notes:


- More than one filter criterion can be used for search. If media asset ID is the filter criterion, other filter criteria are invalid.
- Deleted media assets are displayed only when you search with media asset ID.
- The media asset status can be **Published** or **Unpublished**. The transcoding status can be **Queuing**, **Untranscoded**, **Completed**, or **Failed**.
- The media asset ID is the unique ID for identifying the uploaded source video. Once uploaded, the media asset will have an ID, which is independent of the transcoding status.
- The category ID identifies a category name. You can query the category ID on the **Global settings > Category** page.

Playback

Using this function will incur downstream traffic or bandwidth fees.

- **Preview on the console**
You can preview transcoded video files in MP4, FLV, HLS, and DASH formats on the console. Source video file preview may fail, so transcode them before playing them.

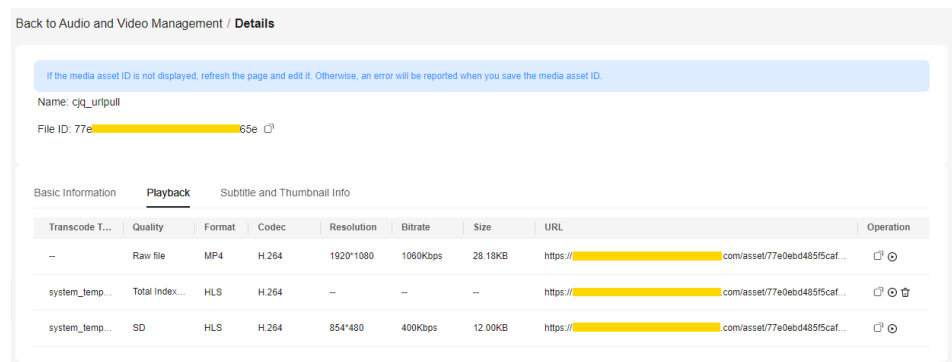
On the **Management > Audio and Video Management** page, you can:

- Click the thumbnail of an audio/video file to preview it.
- Click **Details** on the right of a video. On the page displayed, choose the **Playback** tab and click  in the **Operation** column to preview the video.


NOTICE

H.265 and HLS-encrypted videos cannot be previewed.

Figure 6-6 Playback URL



- **Playback using a player**

Click **Details** on the right of a video. On the page displayed, choose the **Playback** tab. Click  in the **Operation** column to copy the streaming URL and play the video using a player.

When you transcode an audio/video file again,

- if transcoding parameters remain unchanged, the streaming URL remains unchanged.
- if transcoding parameters are modified and
 - the output format is MP4, the previous URL becomes invalid.
 - the output format is HLS or DASH, the primary index URL remains unchanged. The secondary index URL changes and the previous URL becomes invalid.

Deleting Audio/Video Files

To delete one or more audio/video files, select them in the media asset list and choose **More Actions > Delete** above the list. Once deleted, all related resources, including the source file, transcoded file, and snapshot file, will be deleted permanently. The operation cannot be undone. Exercise caution when performing this operation.

6.2 Cold Storage of Media Assets

6.2.1 Cold Storage Based on Media Asset ID

The storage class of media assets can be batch changed from **Standard** to **Infrequent Access** or **Archive** by media asset ID.

Notes

The storage class cannot be changed when a media asset has an ongoing task, such as snapshot capturing or transcoding.

Procedure

- Step 1** Log in to the [VOD console](#).
- Step 2** In the navigation pane, choose **Management > Asset cooling**. The media asset cold storage page is displayed, as shown in [Figure 6-7](#).

Figure 6-7 Media asset cold storage

Asset cooling

Direct cooling

Trigger Condition: Asset ID

Target storage type: infrequently accessed st... ▾

If the asset ID of a file is in the following text box, the infrequently accessed storage cooling policy is triggered.

Enter a maximum of 10 IDs of assets to be cooled. Separate multiple IDs with commas (,).

i The infrequently accessed storage must be stored for at least 30 days. If you delete it or convert it to standard storage in advance, you are still charged for 30 days. Access to infrequent files incurs retrieval fees. [Charging Standard](#)

Submit

See [Table 6-4](#).

Table 6-4 Parameters

Parameter	Description
Trigger Condition	By media asset ID.
Target storage type	The storage class of a media asset can be changed from Standard to Infrequent Access or Archive
Media asset ID text box	Enter the IDs of the media assets on which cold storage will be performed. Use commas (,) to separate a maximum of 10 IDs.

Step 3 Click **Submit**. The batch operation has been completed.

Return to the **Management > Audio and Video Management** page and check whether the storage class of the media files has been changed to **Infrequent Access** or **Archive**.

----End

6.2.2 Intelligent Cold Storage Policies

An intelligent cold storage policy can be created to specify the media asset upload time or storage duration, media asset category, and media asset storage class, and batch perform cold storage on media assets. You need to enable the intelligent cold storage policy after creating it.

Notes

- The storage class of media assets can be batch changed from **Standard** to **Infrequent Access** or **Archive**.
- The storage class cannot be changed when a media asset has an ongoing task, such as snapshot capturing or transcoding.
- The minimum storage period is 30 days for objects of the **Infrequent Access** storage class, and 90 days for those of the **Archive** storage class. If media files are retrieved or deleted before the storage period expires, you will still be charged based on the minimum storage period.
Infrequent Access is used as an example. If the actual storage period is shorter than 30 days, you will be charged based on the minimum storage period (30 days). If the actual storage period is at least 30 days, you will be charged based on the actual storage period.
- Each tenant can execute a maximum of 50,000 cold storage tasks every day.

Procedure

Step 1 Log in to the [VOD console](#).

Step 2 In the navigation pane, choose **Management > Asset cooling**.

Step 3 Choose the **Intelligent cooling policy** tab and click **Create an intelligent cooling policy**.

On the page displayed, configure a policy, as shown in [Table 6-5](#). The policy is executed only for audio/video files that meet all filter criteria.

Table 6-5 Parameters

Category	Parameter	Description
Basic Information and Triggering Conditions	Policy name	Intelligent cold storage policy name. Only letters, digits, and underscores (_) are allowed.
	Media time condition	Conditions for media asset cold storage. Options: <ul style="list-style-type: none"> • Specified upload time: If this option is selected, you need to set the time range for uploading a media asset, including the start time and end time. Media assets uploaded within the time range will adopt cold storage in batches. If only the start time is specified, all media assets uploaded after the start time will adopt cold storage. If only the end time is specified, all media assets uploaded before the end time will adopt cold storage. • Specified storage duration: If this option is selected, you need to set the number of days after media file upload. The policy will be executed after this period.
	Media classification condition	(Optional) Select the media asset category for batch cold storage from the drop-down list box.
	Storage Type	Select the media asset storage class for batch cold storage from the drop-down list box.
Execute Configuration	Target storage type	Storage class after batch media asset cold storage.
	Start Date	Date when the policy takes effect. The date takes effect only after the policy is enabled. Batch cold storage is started at 00:00 (UTC time) on the next day of the effective date.

Step 4 Click **Submit**. The intelligent cold storage policy has been created.

The new intelligent cold storage policy is displayed on the **Intelligent cooling policy** tab under **Management > Asset cooling**.

Step 5 Click the icon in the **Enable/Disable** column of the new intelligent cold storage policy to enable the policy.

After the policy is enabled, media files will batch adopt cold storage at 00:00 (UTC time) on the next day of the effective date.

Return to the **Management > Audio and Video Management** page and check whether the storage class of the media files has been changed to **Infrequent Access** or **Archive**.

----End

7 Video Processing

7.1 Snapshot Capturing

Functions

You can capture snapshots for an uploaded video file by time interval, specific timestamp, or total count. You can use a snapshot as the video thumbnail. You are charged by the number of snapshots.

- Taking snapshots by time interval: The system takes snapshots at regular intervals from the first frame to the last frame. The interval cannot exceed 12 seconds.
- Taking snapshots at fixed time: The system takes snapshots at fixed time points. A maximum of 10 time points can be configured for a video.
- Taking snapshots by total count: The system takes snapshots at equal intervals throughout video based on the specified count.

Constraints

- You can take snapshots from an MP4, TS, MOV, MXF, FLV, MPG, WMV, AVI, M4V, F4V, MPEG, 3GP, ASF, MKV, WEBM, RMVB, VOB, RM, MTS, DV, DAT, QT, M2T, or SWF video.
- Snapshots are saved as JPG files.
- By default, the system operates in the single-snapshot mode. That is, only the most recent snapshot task and its results are displayed for a video, and historical snapshots are overwritten. Consequently, [Figure 7-4](#) only displays the latest snapshot task.
- To retain all snapshot tasks and their snapshot results, you need to [submit a service ticket](#) to enable the multi-snapshot support. Then [Figure 7-4](#) will display all snapshot tasks.

Note the following when using the multi-snapshot function:

- A maximum of 2,000 snapshot tasks can be created for a single media asset.

- If two snapshot tasks for the same media asset share identical parameters, the system will only retain the latest snapshots and overwrite the historical ones by default.
- To query the snapshots captured by a single-snapshot task, you can call the [Querying a Media Asset](#) API. The [Querying Snapshot Details](#) API is used to query snapshots captured by a multi-snapshot task.

Procedure

Step 1 Log in to the [VOD console](#).

Step 2 In the navigation pane, choose **Video Processing > Snapshots**.

Step 3 Locate the target video file and click **Create Snapshot Task** in the **Operation** column. You can also select multiple video files and click **Create Snapshot Task** above the list.

Step 4 Configure video snapshot parameters.

Snapshots can be taken at a specified interval, at a specified time point, or at a specified quantity.

- **By interval**

Figure 7-1 Snapshot settings

Snapshot Settings ✕

i The first frame is taken at 0s. A black screen may be displayed.

Frequency By Interval Specified time point
 Specified quantity

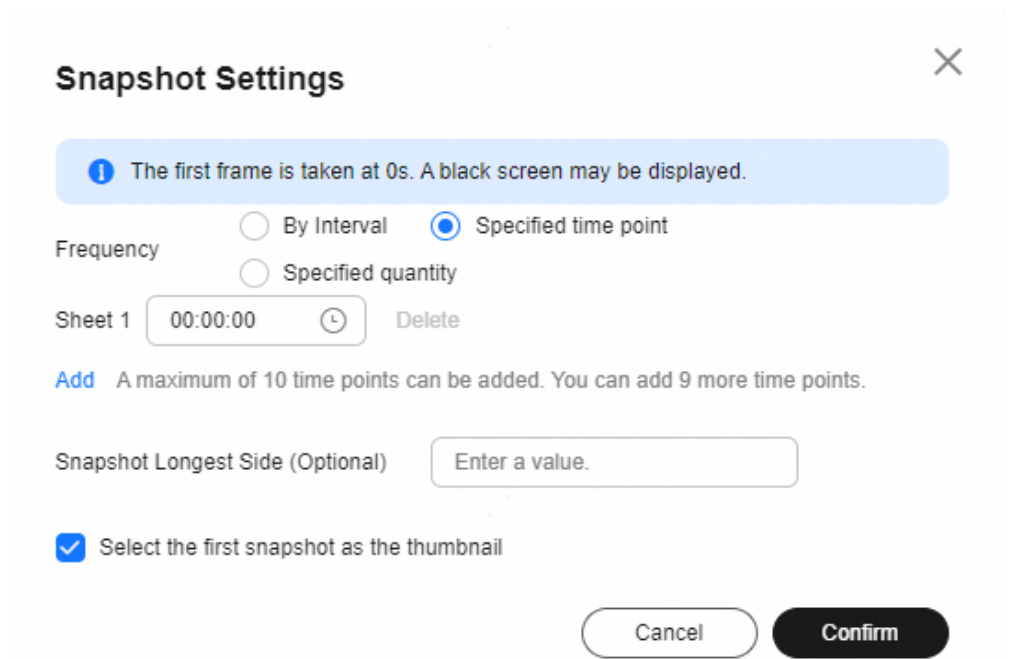
Interval ▾

Snapshot Longest Side (Optional)

Select the first snapshot as the thumbnail

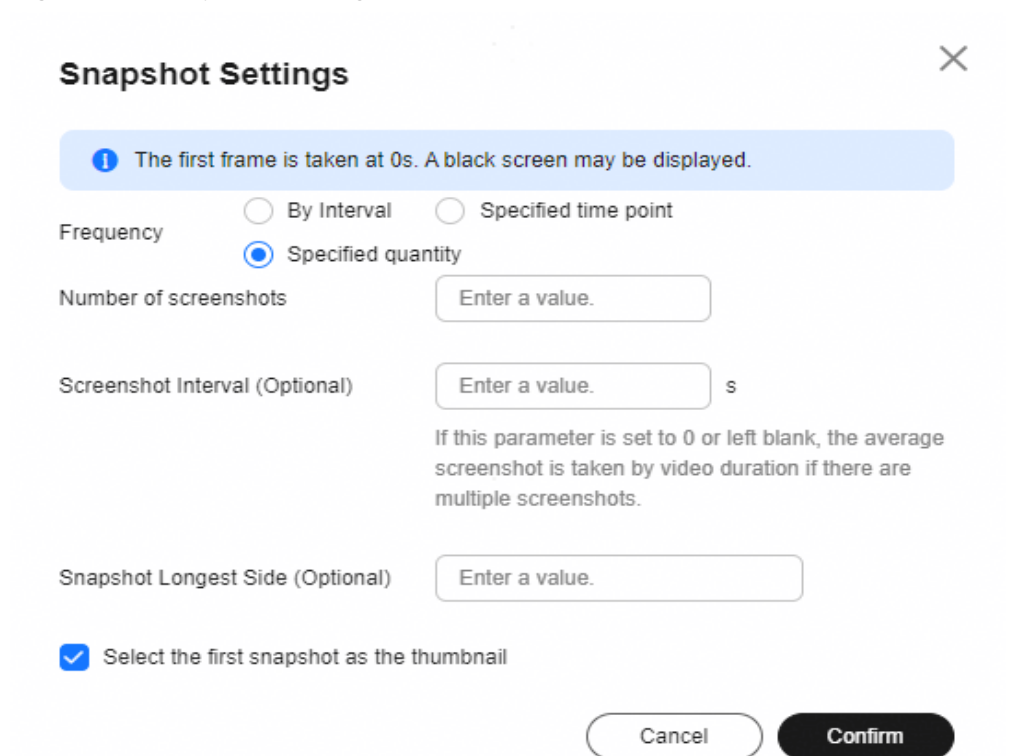
- **At fixed time**

Figure 7-2 Snapshot settings



- Specified quantity

Figure 7-3 Snapshot settings



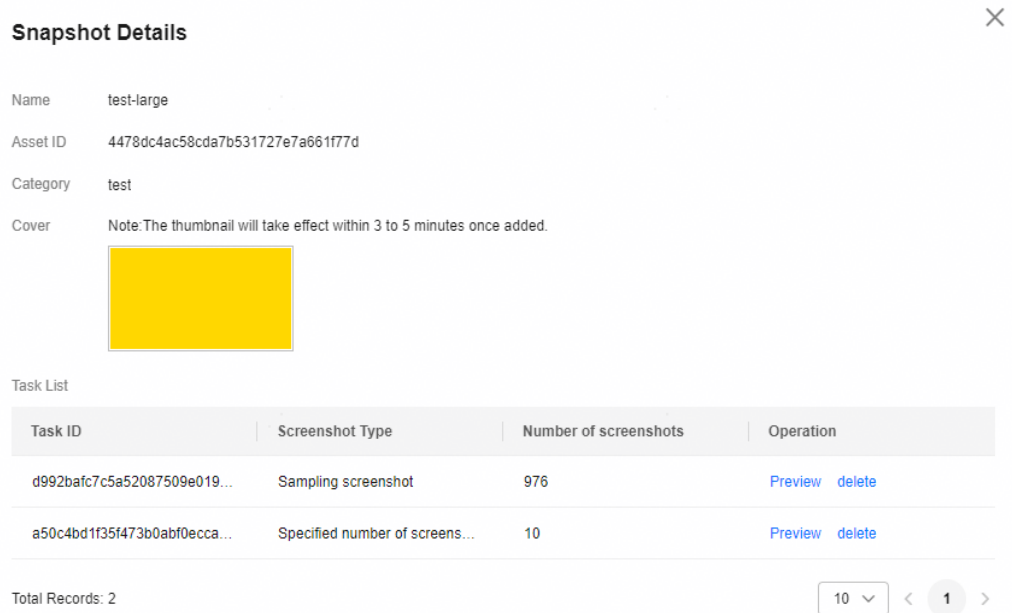
Step 5 Click **OK**.

If video status changes to **Captured**, snapshots have been captured.

Step 6 After snapshots are captured, click **Details** in the **Operation** column to view snapshot details, as shown in **Figure 7-4**.

You can view the video name, media asset ID, media asset category, current thumbnail, and snapshot task list.

Figure 7-4 Snapshot details

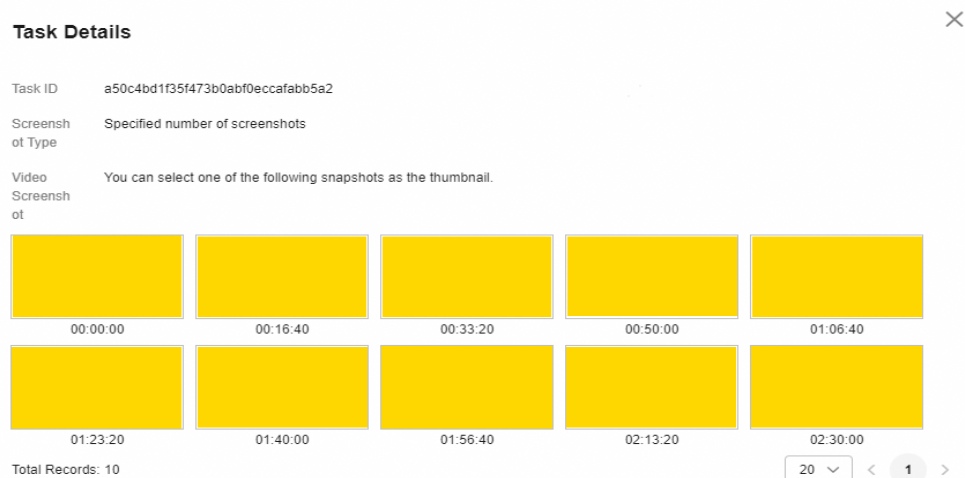


Step 7 View the list of all snapshot tasks created for the video file.

You can perform the following operations on a snapshot task:

- Click **Preview** in the row of the task to open the **Task Details** page, as shown in **Figure 7-5**.
You can view the ID, snapshot type, and all snapshots of the snapshot task. You can select a snapshot as the thumbnail. The new thumbnail takes effect in 3 to 5 minutes.
A maximum of 20,000 snapshots can be previewed. To display more snapshots, [submit a service ticket](#).
- Click **Delete** in the row of the task to delete the task.

Figure 7-5 Task details



----End

7.2 Workflow Management

VOD provides multiple media processing functions such as transcoding, content moderation, snapshot capturing, and audio extraction. A workflow incorporates all these functions to help you process media files faster.

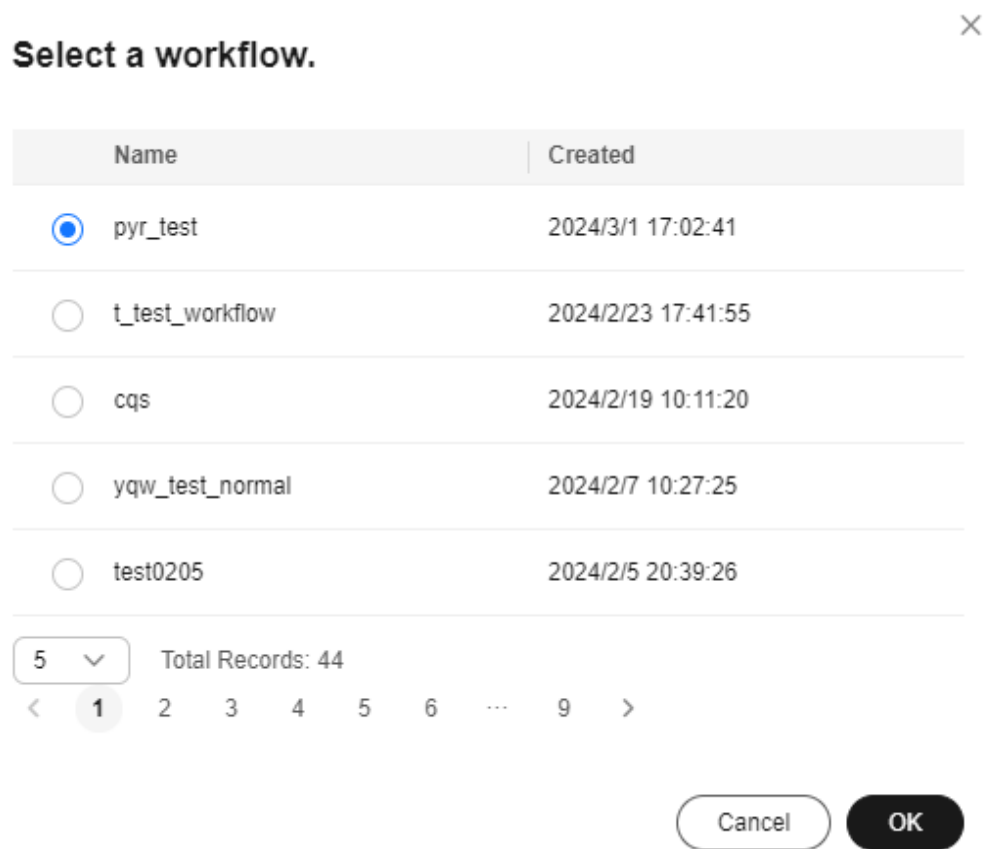
Prerequisites

A workflow has been created. For details, see [Workflow Settings](#).

Procedure

- Step 1** Log in to the [VOD console](#).
- Step 2** In the navigation pane, choose **Video Processing > Workflow Management**.
- Step 3** Locate the target media file and click **Start** in the **Operation** column or select multiple files and click **Start Workflow** above the media list.
- Step 4** Select a workflow and click **OK**.

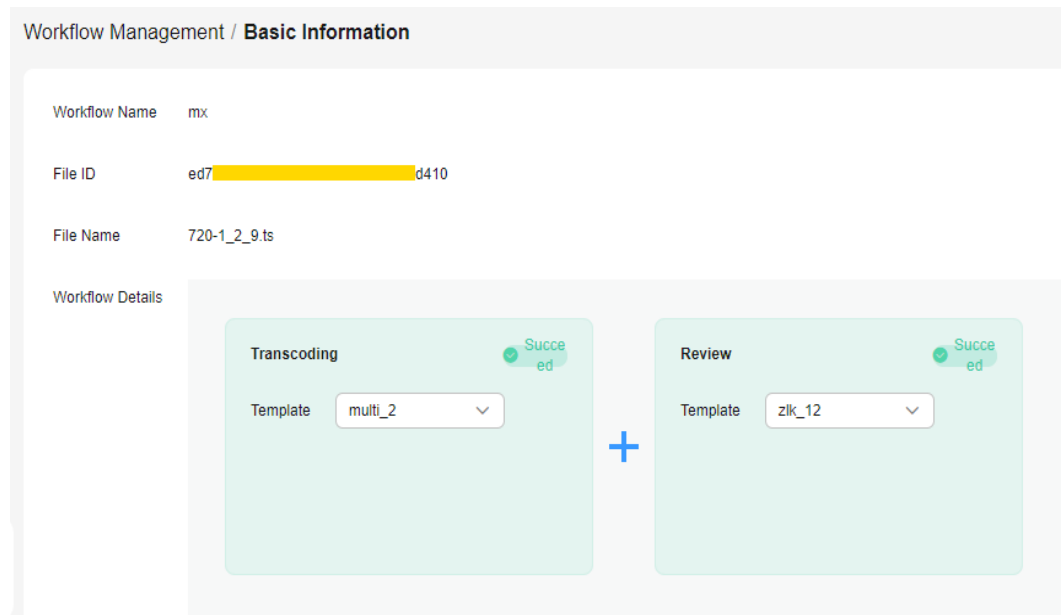
Figure 7-6 Selecting a workflow



Step 5 Click **View** in the **Operation** column to view workflow details.

If the workflow execution fails, you can view the task status and error information, as shown in [Figure 7-7](#).

Figure 7-7 Workflow details



----End

8 Global Settings

8.1 Transcoding Settings

You can transcode an audio/video file during or after upload using one of the four system templates or a custom template. To receive notifications about transcoding results, configure **notifications** before you start transcoding.

Scenarios

Audio and video distributed by VOD may be referenced by product websites and video websites or be played on devices like PCs and smartphones. VOD provides transcoding to change the audio/video encoding format, container format, resolution, and bitrate to adapt to different scenarios, devices, and network environments.

The transcoding function helps you achieve:

- Compatible with different devices. You can transcode the source audio/video into formats such as MP4 for playback on a wide range of devices.
- Adaptation to different network environments. You can set the output bitrate based on the network bandwidth.
- Low distribution costs. H.265 codec and low-bitrate HD can reduce the bitrate by about 20% without changing the resolution, thereby reducing media file distribution costs.
- HLS encryption. You can enable HLS encryption during transcoding to prevent secondary distribution if a media file is stolen.
- Copyright protection. You can add watermarks such as logos to your video.
- Audio extraction. Audio files can be extracted during transcoding. This function is used for those requiring audio only, such as radio stations and audio apps.
- Video extraction. You can disable audio and output video only.

Transcoding Template Introduction

VOD provides four system transcoding templates. If you are a new user of VOD, system templates are recommended.

- **non_transcoding_template_group:** This template does not transcode audios/videos. If you do not select any transcoding template, this template takes effect by default.
- **system_template_group:** In this template, resolution, bitrate, and frame rate are preconfigured. If you are not familiar with these parameters, you are advised to use this template.
- **original_template_group:** This template only changes the audio/video container format.
- **adaptive_template_group:** With image enhancement preconfigured, this template is ideal for repairing corrupt videos.

If you are familiar with audio/video parameters and system templates cannot meet your requirements, you can create a transcoding template.

Notes

- Input audios/videos of the following formats can be transcoded:
 - Supported input audio formats: MP4, TS, MOV, FLV, MPG, MXF, WMV, ADTS, AVI, MKV, MPEG, VOB, RM, and MTS
 - Supported input video codecs: H.264, H.265, MPEG-2, MPEG-4, MJPEG, WMV1/2/3, and ProRes 422
 - Supported input audio codecs: AAC, AC3, EAC3, HE-AAC, MP2, MP3, PCM (s16le, s16be, s24le, s24be, DVD), and WMA
- To retain transcoded outputs of different formats, you need to [submit a service ticket](#).
- If the source file is transcoded successfully but the output video is shorter than the original, this is related to the current transcoding mechanism.
 - If the source contains a short abnormal segment, that segment is dropped. For example, if in a 10-minute video, the content becomes abnormal after minute 9, the transcoded video will be 9 minutes long, with the abnormal final minute removed.
 - If the source contains a long abnormal segment, for example, more than 3 minutes, transcoding will fail.
- If the audio bitrate is set too high when the source file is transcoded to HLS, a black screen will be displayed during playback on iOS devices. You are advised to customize a transcoding template and set a lower audio bitrate to ensure that the audio-to-video bitrate ratio is 1:3.

Editing a System Template

A system template has common parameters such as video resolution and codec preconfigured. Before using a system template, you are advised to check whether the settings of the system template meet your requirements. If the settings do not, you can edit the system template.

Step 1 Log in to the [VOD console](#).

Step 2 In the navigation pane, choose **Global Settings > Transcoding Templates**.

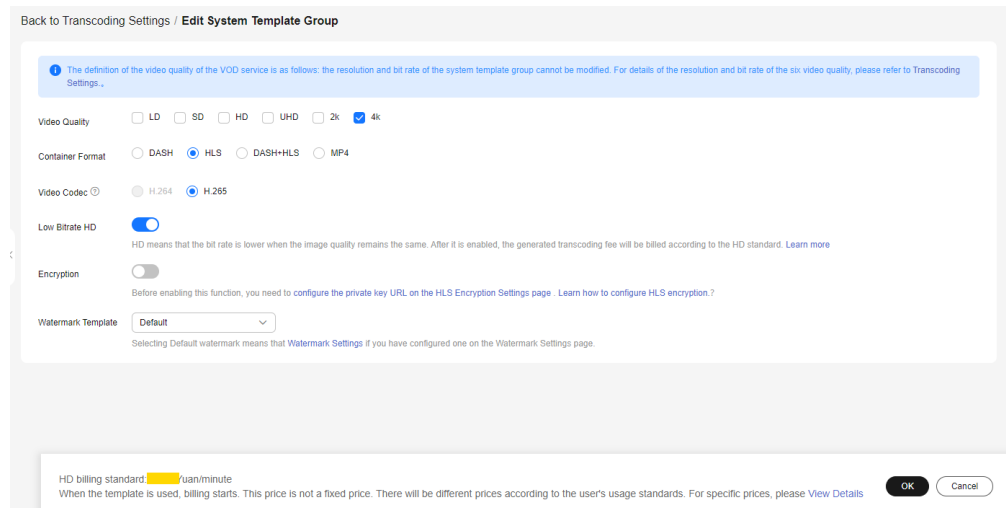
Step 3 Find the desired system template and click **Edit**. On the page displayed, modify template parameters.

The editable parameters vary depending on system templates.

- System template (**system_template_group**)

You can change the video quality, container format, video codec, and watermark template, and enable low-bitrate HD and encryption. **Video Quality** has six options: LD, SD, HD, UHD, 2K, and 4K, as shown in [Table 8-3](#).

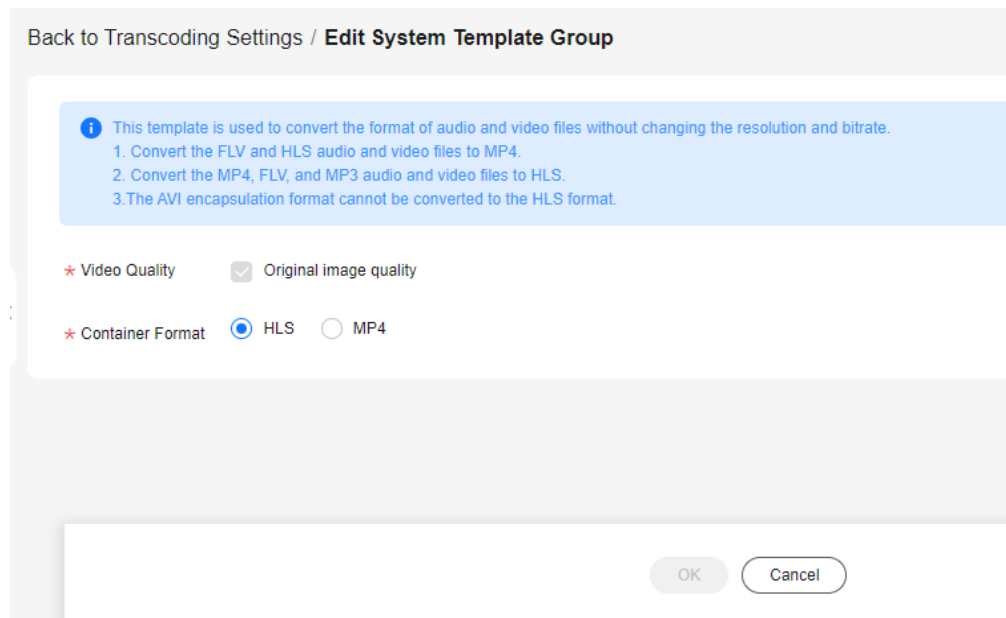
Figure 8-1 System template



- Container template (**original_template_group**)

You can change the format from FLV/HLS to MP4, or from MP3/MP4/FLV to HLS.

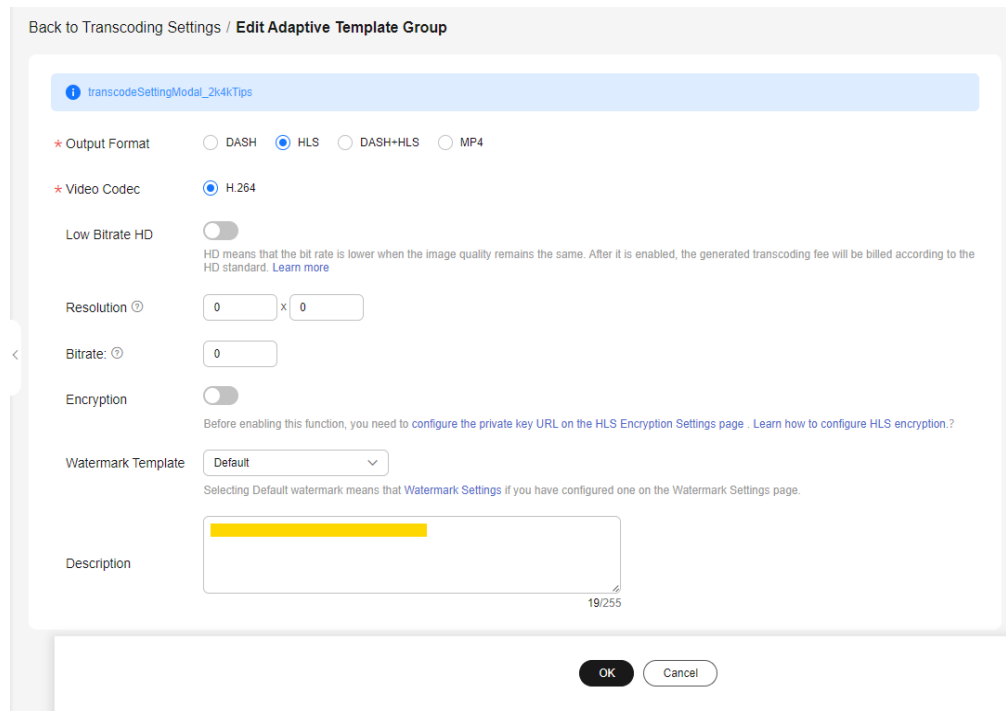
Figure 8-2 Container template



- Adaptive template (**adaptive_template_group**)

Video codec can only be H.264. You can change the resolution. If the resolution is not set, the input resolution is used by default. After enabling low-bitrate HD, you can use video enhancement.

Figure 8-3 Adaptive template



Step 4 Click **OK**.

----End

Creating a Template Group

If the preset templates cannot meet your requirements, you can create a template based on your needs. To customize an audio transcoding template, select **MP3** or **ADTS** for **Output Format**.

Step 1 Log in to the [VOD console](#).

Step 2 In the navigation pane, choose **Global Settings > Transcoding Templates**.

Step 3 Click **Create Custom Template Group**. In the dialog box displayed, specify related parameters.

Step 4 Set **Basic Information** by referring to [Figure 8-4](#) and [Table 8-1](#).

Figure 8-4 Setting basic information

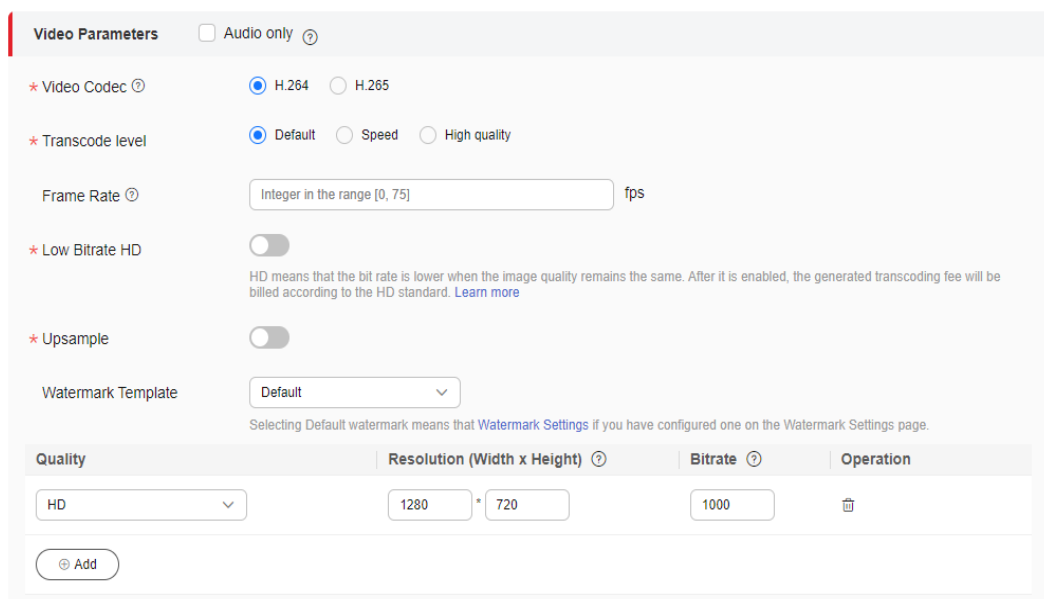
Table 8-1 Parameters

Parameter	Description
Name	A template name can contain a maximum of 128 characters in letters, underscores (_), and digits. Example: MP4_H264
Description	Description of a custom template.
Output Format	<ul style="list-style-type: none"> Supported video formats: MP4, HLS, DASH_HLS, and DASH Supported audio formats: ADTS and MP3 Note: If an audio format is selected, video parameters are disabled.
Package Format	Video container format. This parameter is available only when Output Format is set to HLS or DASH_HLS . Options: <ul style="list-style-type: none"> TS FMP4
Segment Duration (s)	HLS segment length. This parameter is available only when Output Format is set to HLS or DASH_HLS .

Parameter	Description
Different Segment Durations	<p>Whether to enable variable-length segmentation, which controls playback startup time after transcoding.</p> <p>This parameter is available only when Output Format is set to HLS or DASH_HLS.</p> <p>If this function is enabled, you also need to set the following parameters:</p> <ul style="list-style-type: none"> • Initial Short Segments: specifies the number of segments before a video starts to play. The value is an integer ranging from 1 to 10. • Short Segment Duration: specifies the duration of each initial short segment. The value is an integer ranging from 1 to 10, in seconds. <p>After these parameters are configured, playback can start more quickly.</p>
Maximum I-Frame Interval	<p>Maximum I-frame interval.</p> <p>The value ranges from 1 to 10, in seconds.</p> <p>Default value: 5</p>
Encryption	<p>Whether to encrypt output media files. Input audio/video files are not encrypted. This parameter is available only when Output Format is set to HLS. That is, only HLS audio/video files can be encrypted and output. Before enabling this function, obtain the key URL by referring to HLS Encryption Settings.</p>

Step 5 Configure **Video Parameters** by referring to [Figure 8-5](#) and [Table 8-2](#).

Figure 8-5 Video parameters



 NOTE

If **Audio only** is selected, the output files do not contain any video information. Use this option to extract audio from a video file. Then perform [7](#) to configure audio parameters.

Table 8-2 Video parameters

Parameter	Description
Video Codec	H.264 and H.265 are available.
Transcode level	Video encoding quality level. Options: <ul style="list-style-type: none">• Default: The default mode is used.• Speed: Efficiency is prioritized.• High quality: Transcoded video quality is prioritized.
Frame Rate	Number of frames displayed per second. The value is an integer ranging from 0 to 75. If the value is set to 0 or 1 , the transcoded and input videos have the same frame rate.
Low Bitrate HD	Whether to enable low-bitrate HD. Low-bitrate HD means achieving the same image quality with a lower output bitrate. If this function is enabled, the transcoding fee will be charged based on the low-bitrate HD standard. For details, see VOD Pricing Details .
Upsample	Enabling this function improves video resolution and increases the number of sampling points.
Watermark Template	Select the default watermark template or a custom watermark template. <ul style="list-style-type: none">• Select Default to use the default watermark template set in Watermark Settings.• Select a custom watermark template to be used during transcoding.
Stream Name	Stream name of a transcoded video.
Quality	Video quality. The options are 4K, 2K, UHD, HD, SD, and LD.
Resolution (Width x Height)	The default value is the recommended resolution for your selected video quality. You can change it based on your needs. <ul style="list-style-type: none">• If the width or height is set to 0, the side set to 0 is scaled in proportion to the other side.<ul style="list-style-type: none">– When the width is 0 and the height is not, the width is scaled proportionally.– When the height is 0 and the width is not, the height is scaled proportionally.• If both the width and height are 0, the transcoded file uses the resolution of the input file.

Parameter	Description
Bitrate	The default value is the recommended bitrate for your selected video quality. You can change it based on your needs. If the bitrate is set to 0 , the recommended bitrate for your input file is used for output.

 **NOTE**

- There can be up to six outputs at different resolutions.
- If you change the default resolution for an output stream, you are billed based on the configured resolution. For details, see [VOD Pricing Details](#).

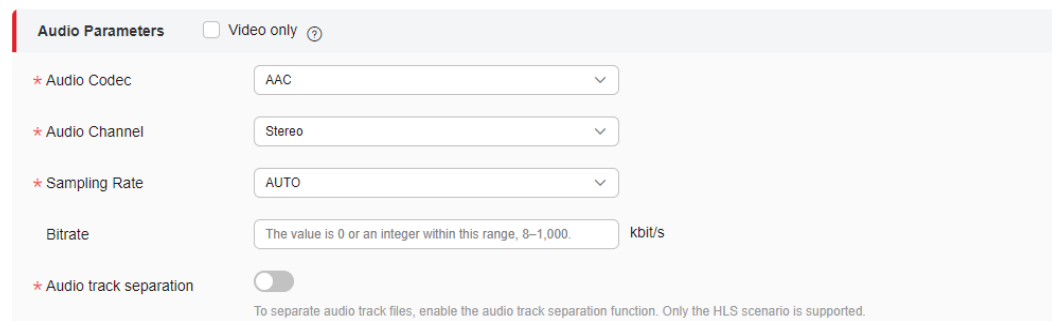
You are advised to use the recommended resolutions and bitrates. For details, see [Table 8-3](#).

Table 8-3 Recommended resolutions and bitrates

Video Quality	Recommended Resolution	Recommended Bitrate for H.265 (kbit/s)	Recommended Bitrate for H.264 (kbit/s)
4K	3840 x 2160	5,600	8,000
2K	2560 x 1440	4,900	7,000
UHD	1920 x 1080	2,100	3,000
HD	1280 x 720	700	1,000
SD	854 x 480	500	600
LD	480 x 270	200	300

Step 6 Configure **Audio Parameters** by referring to [Figure 8-6](#) and [Table 8-4](#).

Figure 8-6 Audio parameters



 NOTE

If **Video only** is selected, the output file does not contain any audio information. This option is used for video extraction from a media file.

Table 8-4 Audio parameters

Parameter	Description
Audio Codec	Audio codec. AAC and HEAAC1 are available. The default value is AAC .
Audio Channel	Number of audio sources during audio recording or number of speakers during audio playback. Stereo and Mono are available. The default value is Stereo .
Sampling Rate	Number of times per second that the audio signal is sampled. AUTO, 22050, 32000, 44100, 48000, and 96000 are available. The default value is AUTO , and the unit is Hz.
Bitrate	Bitrate of an output audio, in kbit/s. The value is 0 or an integer ranging from 8 to 1,000. If this parameter is set to 0 , the audio bitrate is an adaptive value. As a result, the audio bitrate of the transcoded file may be greater than that of the input video. So set this parameter to a proper value other than 0 . CAUTION If the audio bitrate is set too high when the source file is transcoded to HLS, a black screen will be displayed during playback on iOS devices. You are advised to customize a transcoding template and set a lower audio bitrate to ensure that the audio-to-video bitrate ratio is 1:3.
Audio track separation	If the audio track file needs to be separated from the video file, toggle on this switch. This function is applicable only to HLS. The audio in the transcoded file is stored separately. NOTICE The Audio track separation and Customize the primary index file options are mutually exclusive. You can configure only one of them.

Step 7 Customize the primary index file, as shown in [Figure 8-7](#). [Table 8-5](#) describes the parameters you need to configure.

NOTICE

- If **Disable the file name extension of the primary index** is selected, you do not need to set the parameters.
- You can customize the primary index file only when **Output Format** is set to **HLS**.
- The **Audio track separation** and **Customize the primary index file** options are mutually exclusive. You can configure only one of them.

Figure 8-7 Customizing the primary index file

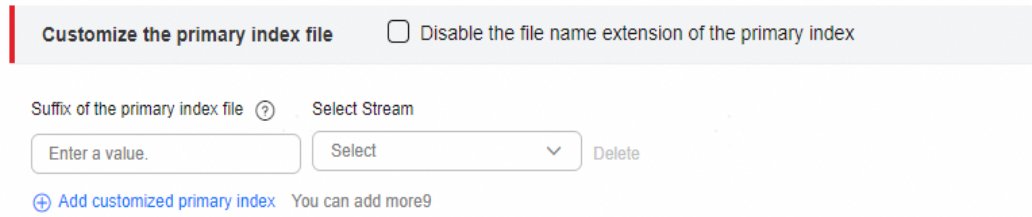


Table 8-5 Parameters for customizing the primary index file

Parameter	Description
Suffix of the primary index file	The name of the primary index file is index_{suffix} .
Select Stream	By default, the drop-down list displays all stream names added. Select one or more stream names as required.

Step 8 Click **OK**.

You can view the created template on the **Transcoding Settings** page.

----End

Editing or Deleting a Custom Template

After a custom template is created, you can click **Edit** in the template list to modify the template. You can also click **Delete** to delete templates that you no longer need. If a template is deleted, audio/video using this template will not be deleted.

Figure 8-8 Editing a custom template

Transcoding Templates

Note: You can set a template group as the default template group. The default template is used for each video upload and transcoding. For details, see [Transcoding Settings](#). For the price of transcoding, see [Pricing Details](#). Low bit rate will cause the video to appear flowery screen or unable to play.

Note: Transcoding package FHD(1920x1080),HD(1280x720),SD(640x480),their transcoding duration are calculated based on the ratio of 3:1.5:1, for example,once the FHD (1920x1080) transcoding duration is converted into three times the SD (640x480) transcoding duration, and once the HD (1280x720) transcoding duration is converted into 1.5 times the SD (640x480) transcoding duration.

Create Custom Template Group

Name	Type	Description	Operation
non_transcoding_template_group	System template group	Non-transcoding template	
system_template_group	System template group	Video transcoding template. The resolution and bit...	Edit
original_template_group	System template group	This template only converts the format. It does not...	Edit
adaptive_template_group	System template group		Edit
mmxx	Custom template group		Edit Delete
cjq_330_test	Custom template group		Edit Delete
ajgsvd	Custom template group		Edit Delete
03251	Custom template group		Edit Delete
his_audio	Custom template group		Edit Delete
volvo_MP4	Custom template group		Edit Delete

10 Total Records: 125 < 1 2 3 4 5 6 ... 13 >

8.2 Watermark Settings

You can upload an image and position it wherever you want your watermark to appear on your video.

Notes

- Watermarks can only be added to videos through transcoding. Therefore, adding watermarks will incur transcoding fees.
- If you do not need to add watermarks, set all watermark templates as non-default before transcoding, and select the default watermark in a transcoding template.
- If you cannot preview the watermark image, check the [domain name configuration](#).

Constraints

- You can create a maximum of two watermark templates. That is, a maximum of two watermarks can be added to a video.
- Requirements for watermarks are as follows:
 - Watermarks can be PNG, JPG, or JPEG.
 - The resolution of a watermark must be between 8x8 and 4096x4096. The image size cannot exceed 10 MB.

Creating a Watermark Template

- Step 1** Log in to the [VOD console](#).
- Step 2** In the navigation pane, choose **Global Settings > Watermark Templates**.
- Step 3** Click **Create Watermark**. On the page displayed, configure watermark parameters.

Figure 8-9 Configuring watermark parameters

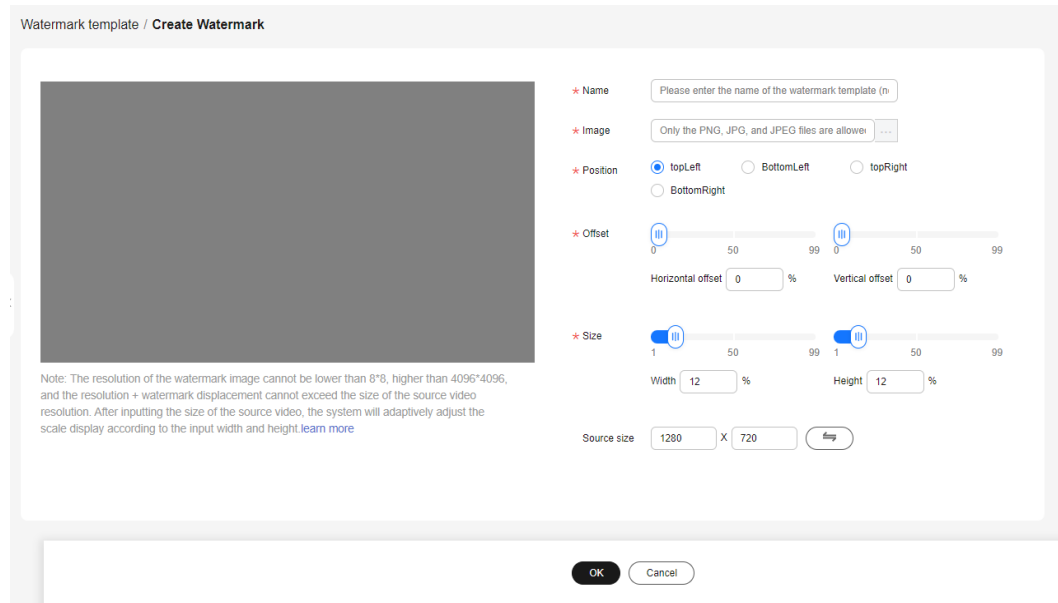


Table 8-6 Parameters

Parameter	Description
Name	Enter a maximum of 64 characters.
Image	Only a PNG, JPG, or JPEG image no larger than 10 MB is allowed. The transparent PNG format is recommended.
Position	Initial position of the watermark, which defaults to upper right.
Offset	Set the horizontal or vertical offset based on the initial position.
Size	Size of the watermark image, which is zoomed in or out based on the preset ratio.
Source size	You can preview the watermark layered on the video.

- Step 4** View the watermark in the preview area on the left.
- Step 5** Click **OK**. The new template is added to the watermark template list.
- Step 6** Click **Set as Default** in the **Operation** column to set a watermark template as a default one.

After the default watermark is set, **Default** is selected for **Watermark Template** by default. If you do not change it, the default watermark is added to videos. For details, see [Transcoding Settings](#).

NOTICE

If you only need to add watermarks to some videos, you are advised to use a custom template instead of the default template.

----End

8.3 Security Settings

8.3.1 HLS Encryption Settings

Hotlink protection prevents unauthorized users from downloading and playing videos, but cannot prevent malicious paid users from downloading videos to their local PCs for secondary distribution. For this purpose, VOD provides HLS encryption. Encrypted videos cannot be distributed to others even if they are downloaded by malicious users.

 **NOTE**

For details about HLS encryption, see [Protecting Videos with HLS Encryption](#).

Notes

- HLS encryption must be performed through transcoding, so transcoding fees are generated for HLS encryption.
- VOD does not encrypt HLS inputs. It encrypts HLS outputs except for those in MP4 and DASH formats.
- Encryption and decryption comply with HLS specifications. Only players that support HLS streams can play the content.
- If the URL for obtaining the key is changed, you need to re-encrypt the video. Otherwise, the new encryption key does not take effect.
- If the streaming URL used after encryption is HTTPS, the KMS URL must also be HTTPS. Otherwise, the video cannot be previewed on the VOD console.

Prerequisites

The Key Management Service (KMS) and token generation service have been deployed. For details, see [Protecting Videos with HLS Encryption](#).

Procedure

- Step 1** Log in to the [VOD console](#).
- Step 2** In the navigation pane, choose **Global Settings > Security**.
- Step 3** Click **HLS Encryption Settings**. On the displayed page, enter the URL for obtaining the key. See [Figure 8-10](#).

Figure 8-10 Encryption settings



Key URL: Enter the KMS address obtained in Prerequisites. HTTPS is recommended, as it is more secure than HTTP.

Example: `https://domain-sample/get-key`

Step 4 Click **OK**.

Step 5 After the configuration is complete, you need to use the **transcoding** function to encrypt video files. HLS encryption must be enabled for the transcoding template.

----End

8.4 Tenant Settings

Media asset cold storage can be set by tenant. Cold storage can be applied only to the source media asset file, or to the entire media asset file (including the source and the transcoded files).

Procedure

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

Step 2 In the navigation pane, choose **Global Settings > Tenant Settings**.

Configure the parameters by referring to **Table 8-7**.

Figure 8-11 Tenant settings

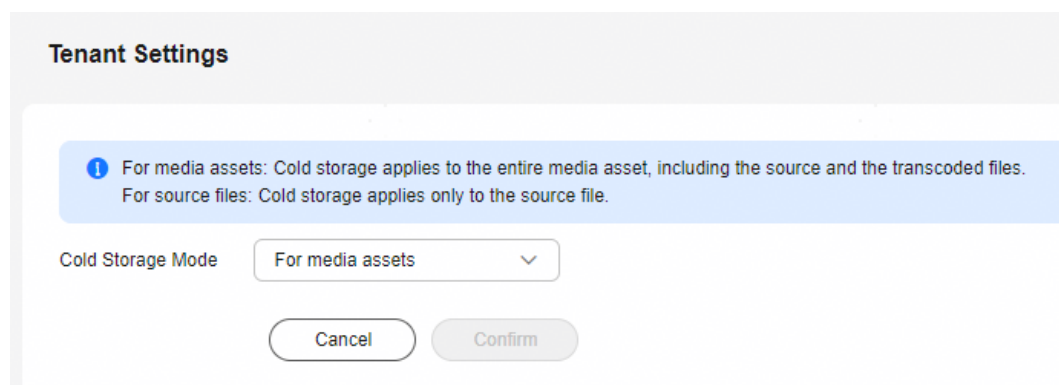


Table 8-7 Parameters

Parameter	Description
Cold Storage Mode	<p>Sets the media asset cold storage mode. Options:</p> <ul style="list-style-type: none"> • Entire media assets: Storage tiering applies to entire media assets, including source and transcoded files. • Source files only: Storage tiering applies only to source files. <p>Default value: Entire media assets</p>

Step 3 Click **Confirm**.

----End

8.5 Authorizing Access to an OBS Bucket

You can authorize VOD to access the media resources you created in the OBS buckets.

Notes

- By default, the **Global Settings > Bucket Authorization** menu is not displayed. To display it, [submit a service ticket](#).
- VOD only reads and writes resources in the authorized OBS buckets, but does not delete input files from the OBS buckets.
- If bucket authorization is canceled, you cannot manage the files that have been synchronized to VOD or play these files on the VOD console.

Procedure

Step 1 Log in to the [VOD console](#).

Step 2 In the navigation pane, choose **Global Settings > Bucket Authorization**. You can see the created OBS buckets.

Step 3 Click **Authorize** on the right of the desired bucket to authorize access to it under the current account.

----End

8.6 Category Settings

You can categorize audio and video files so that you can quickly find them by category. You can also call an API for [creating a media category](#) to categorize media files.

Constraints

- You can add up to 128 categories.

- You can add up to three levels of subcategories.
- If no category is set, the uploaded media files fall into the **Other** category by default.

Adding a Category

Step 1 Log in to the [VOD console](#).

Step 2 In the navigation pane, choose **Global Settings > Categories**.

Step 3 Click **Add** to add a category.

Figure 8-12 Adding a category

Name	Category ID	Operation
673834199292	136978	Delete Add Subcategory Categorize Video
673858254877	136979	Delete Add Subcategory Categorize Video
674869393757	137027	Delete Add Subcategory Categorize Video
675849783188	137097	Delete Add Subcategory Categorize Video
680772409588	137596	Delete Add Subcategory Categorize Video
687145305438	138396	Delete Add Subcategory Categorize Video
689650948572	138753	Delete Add Subcategory Categorize Video
Other	-1	Categorize Video

⊕ Add

Step 4 Click **Add Subcategory** in the row containing the created category to create a subcategory.

Step 5 Categorize audio and video files on the [Audio and Video Management](#) page or during **upload**.

Then, you can click **Categorize Video** to view all files under this category.

Step 6 Click **Delete** to delete an unwanted category.

The rules for deleting a category and subcategory are different:

- If you are going to delete a subcategory, files under this subcategory will be added to its category.
- If you are going to delete a category, files under this category will be added to the **Other** category.

----End

8.7 Notifications

8.7.1 Overview

VOD sends notification messages to notify you of the execution status of tasks such as transcoding and snapshot capturing in real time.

Currently, two notification services are available: MFS and SMN. If you are a new user, MFS is used by default. To use SMN, [submit a service ticket](#).

⚠ CAUTION

The callback message forwarding mode can be switched only when you have modified the callback message logic.

Comparison Between MFS and SMN

The following table lists the differences between MFS and SMN.

Table 8-8 Service differences

Difference	MFS	SMN
Region restriction	MFS is not supported in CN North-Beijing1 and CN East-Shanghai2.	None
Timeliness	High, usually within 5 minutes.	Medium. Queuing occurs during global peak hours, and a delay of more than 10 minutes occurs occasionally.
Billing	Free of charge	SMN charges you for messages. For details, see SMN Pricing Details .
Notification mode	Only REST messages can be sent.	Multiple types of messages, such as SMS messages, emails, and REST messages, can be sent.
JSON message body	Figure 8-13 shows an example of JSON message body.	Figure 8-14 shows an example of JSON message body.

Figure 8-13 JSON message body of MFS

```

JSON
{
  message_id : "1e60bdb99eba4feab9c6de5506c55df7"
  subject : "createComplete"
  message : {"event_type": "createComplete", "create_info": {"status": "SUCCEED", "title": "lcu8qu"}
  timestamp : "1673597532021"
}
    
```

Figure 8-14 JSON message body of SMN

```
JSON
{
  "signature": "HYzplfyCFyUGHrQ8fBQCnnV9ivX5HI++S3gR4WRKPmeqS1/44W9jYy/+so+3xPkAnLyX6AIkbLcWki",
  "subject": "parseComplete",
  "topic_urn": "urn:smn:cn-north-4:0df71765d28090622f97c003c9647a98:Vod-Complete-Topic",
  "message_id": "fb026d9b566a40afa21f42539acd0213",
  "signature_version": "v1",
  "type": "Notification",
  "message": "{\"event_type\":\"parseComplete\",\"parse_info\":{\"status\":\"SUCCEED\",\"asset_id\":\"7d240\", \"unsubscribe_url\": \"https://console.huaweicloud.com/smn/subscription/unsubscribe?region=cn-n\", \"signing_cert_url\": \"https://smn.cn-north-4.myhuaweicloud.com/smn/SMN_cn-north-4_b98100ca131\", \"timestamp\": \"2023-01-06T06:37:20Z\""}",
  "unsubscribe_url": "https://console.huaweicloud.com/smn/subscription/unsubscribe?region=cn-n",
  "signing_cert_url": "https://smn.cn-north-4.myhuaweicloud.com/smn/SMN_cn-north-4_b98100ca131",
  "timestamp": "2023-01-06T06:37:20Z"
}
```

8.7.2 MFS

Message notifications of MFS are free of charge.

NOTICE

MFS is not supported in CN North-Beijing1 and CN East-Shanghai2.

Configuring Notifications

Step 1 Log in to the [VOD console](#).

Step 2 In the navigation pane, choose **Global Settings > Notification Settings**.

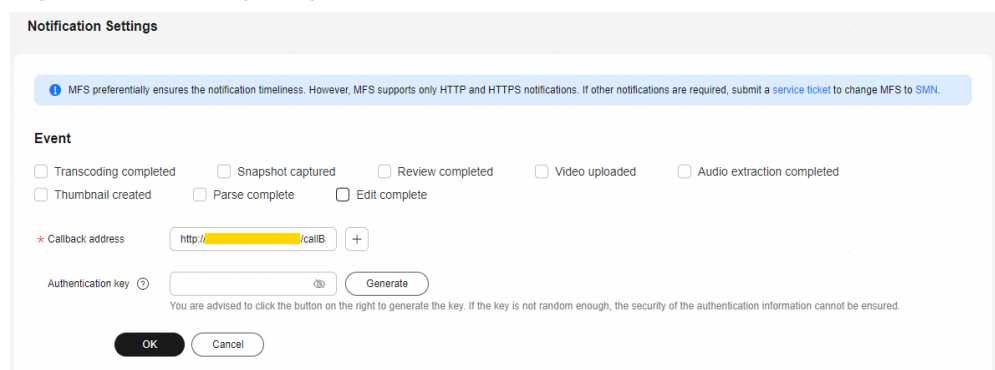
1. Select desired events and enter the callback address.
2. (Optional) If authentication is required, click **Generate** to generate an authentication key.

[MFS Notification Authentication Process](#) shows the message notification authentication process.

NOTICE

If you select both **Snapshot captured** and **Thumbnail created**, only **Snapshot captured** will trigger notifications.

Figure 8-15 Configuring notifications



MFS supports only REST messages. For details about the JSON message template, see [Table 8-9](#).

Table 8-9 JSON message

Parameter	Description	Type
event_type	Event type. The options are as follows: <ul style="list-style-type: none"> • transcodeComplete: transcoding (encryption) completed • thumbnailComplete: snapshot captured • reviewComplete: review completed • createComplete: media file created • audioExtractComplete: audio extracted • coverComplete: thumbnail created • parseComplete: media file parsed • editComplete: media file edited 	String
transcode_info	Transcoding (including encryption) message. For details, see Transcoding Message Body .	TranscodeInfo
thumbnail_info	Snapshot message. For details, see Snapshot Message Body .	ThumbnailInfo
review_info	Review message. For details, see Review Message Body .	ReviewInfo
create_info	Media file upload message. For details, see Media Upload and Audio Extraction Message Body .	AssetInfo
audio_extract_info	Audio extraction message. For details, see Media Upload and Audio Extraction Message Body .	AssetInfo
cover_info	Thumbnail message. For details, see Thumbnail Message Body .	CoverInfo
parse_info	Media file parsing completion message. This parameter is available only when a media file has been parsed. For details, see Media Asset Parsing Message Body .	ParseInfo
edit_info	Media file editing completion message. This parameter is available only when a media file has been edited. For details, see Media Asset Editing Message Body .	ParseInfo

Step 3 Click **OK**.

----End

MFS Notification Authentication Process

The MFS notification authentication process is as follows:

1. VOD generates a timestamp based on the current time and uses the key configured in [Step 2.2](#) to calculate the signature string using `HmacSHA256(VOD_{timestamp}_{body}, key)`.

The signature string and timestamp are sent to the device in the HTTP message header, which is `header[auth_sign]` and `header[auth_timestamp]`, respectively. In the preceding information, `body` indicates the message attribute in the message body.

2. After receiving the response, the customer combines strings in the `VOD_{timestamp}_{body}` format and uses the key in the message header to check whether the signature string generated in `HmacSHA256(VOD_{timestamp}_{body}, key)` is the same as that in the message header. If they are the same, the authentication is successful.

The following is the corresponding Java sample code:

```
//Timestamp, which is the header[auth_timestamp] parameter in the message header.
long reqTime = 1L;
//Message attribute in the message body.
String message = "";
//Key
String key = "";
String algorithm = "HmacSHA256";
//Generate an HmacSHA256 key.
SecretKeySpec signingKey = new SecretKeySpec(key.getBytes(StandardCharsets.UTF_8), algorithm);
// Create a Mac object and initialize it.
Mac mac = Mac.getInstance(algorithm);
mac.init(signingKey);
String content = "VOD."+reqTime+"_"+message;
//Execute HmacSHA256 encryption.
byte[] rawHmac = mac.doFinal(content.getBytes(StandardCharsets.UTF_8));
//Convert the encryption result into a hexadecimal string.
StringBuilder sign = new StringBuilder();
for(byte b : rawHmac) {
    sign.append(String.format("%02x", b));
}
System.out.println(sign);
```

8.7.3 SMN

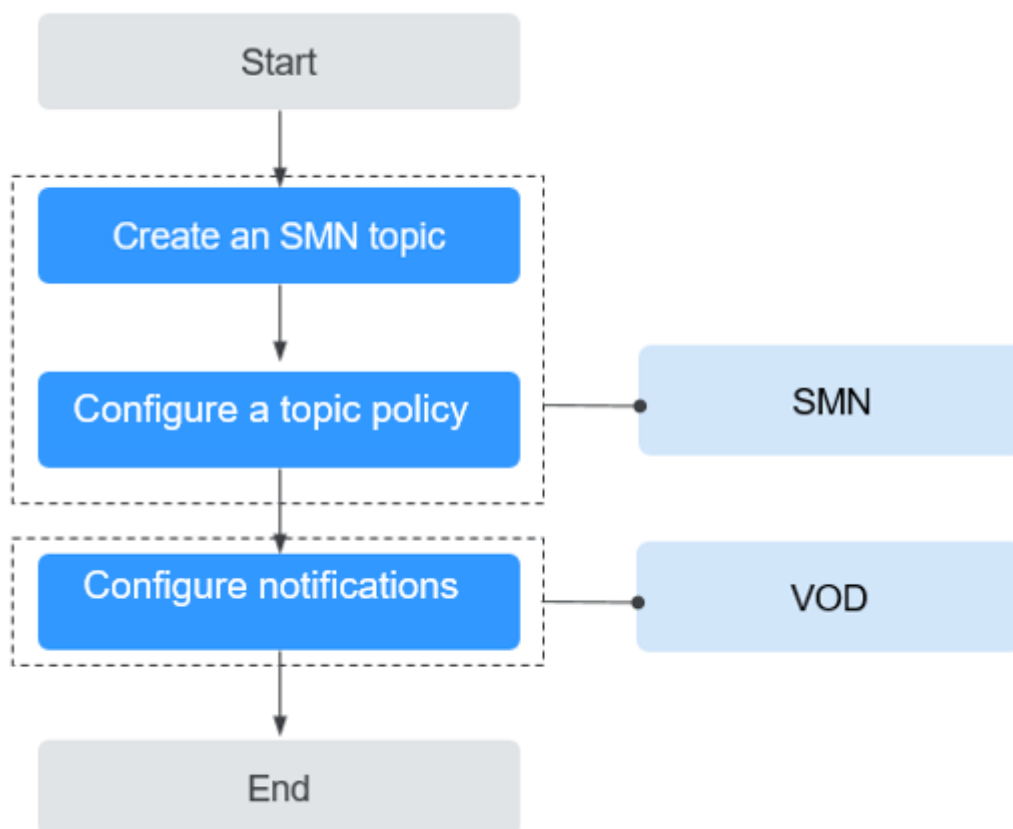
SMN charges messages separately. For details, see [SMN Pricing Details](#).

Function Description

- A topic is used to publish messages and subscribe to notifications. It serves as a message sending channel, where publishers and subscribers can interact with each other. Before configuring notifications, you must create a topic.
- VOD notification types include **Transcoding completed**, **Snapshot captured**, **Review completed**, **Video uploaded**, **Audio extraction completed**, and **Thumbnail created**. Subscription is to associate a subscriber to a topic. A user can have multiple topics, and each topic has multiple subscribers.

Process Flow

[Figure 8-16](#) shows the process of configuring notifications.

Figure 8-16 Process of configuring notifications

1. **Create an SMN Topic** on the SMN console.
2. **Configure a topic policy** to authorize VOD to publish messages to the topic.
3. **Configure notifications** on the VOD console so that you can receive notifications during operations such as transcoding, snapshot capturing, and review.

Creating an SMN Topic

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

Step 2 In the navigation pane on the left, choose **Topic Management > Topics**.

Step 3 Click **Create Topic** in the upper right corner.

The **Create Topic** dialog box is displayed. **Table 8-10** describes the required parameters.

Table 8-10 Topic parameters

Parameter	Description
Topic Name	Specifies the topic name, which <ul style="list-style-type: none"> • Contains only letters, digits, hyphens (-), and underscores (_), and must start with a letter or digit. • Contains 1 to 255 characters. • Must be unique and cannot be modified after the topic is created.
Display Name	This parameter is optional. When sending an email: <ul style="list-style-type: none"> • If the display name is not specified, the sender is displayed as <i>username@example.com</i>. • If the display name is specified, the email sender is presented as <i>Display name<username@example.com></i>.
Enterprise Project	Centrally manages cloud resources and members by project.
Tag	Specifies a key-value pair. Tags identify cloud resources so that you can easily categorize and search for your resources.

Step 4 Click **OK**.

Step 5 Click **Add Subscription** in the **Operation** column of the new topic. The **Add Subscription** dialog box is displayed.

Configure the subscription protocol and endpoints based on [Table 8-11](#).

Table 8-11 Subscription parameters

Parameter	Description
Topic Name	Name of the topic to be subscribed to. Retain the default value.
Protocol	Message notification method. Select a protocol from the drop-down list. The common protocols used by MPC are SMS , Email , HTTP , and HTTPS .

Parameter	Description
Endpoint	<p>Specifies the IP address of a subscription endpoint. You can enter up to 10 SMS, email, HTTP, or HTTPS endpoints, one in each line.</p> <ul style="list-style-type: none"> SMS: Enter one or more valid phone numbers. The format is + <i>country code phone number</i>, for example, +8600000000000. <p>Subscribers will receive a subscription confirmation message valid for 48 hours and must confirm the subscription to receive messages published to the topic.</p> Email: Enter one or more valid email addresses, for example, <i>username@example.com</i>. <p>Subscribers will receive a subscription confirmation email valid for 48 hours and must confirm the subscription to receive messages published to the topic.</p> If you select HTTP or HTTPS, enter a public network address and confirm the subscription, for example, https://example.com/notification/action. <p>HTTPS is recommended, as it is more secure than HTTP.</p>

Step 6 Click **OK** to add a subscription. You can view the subscription on **Topic Management > Subscriptions**.

After the subscription is added, the configured subscription endpoint will receive a subscription confirmation message. The subscription confirmation link is valid for 48 hours. You need to confirm the subscription within the validity period so that you can receive messages published to the topic.

----End

Configuring a Topic Policy

Step 1 Go to the [SMN console](#).

Step 2 In the navigation pane on the left, choose **Topic Management > Topics**.

Step 3 Choose **More > Configure Topic Policy** in the **Operation** column of the created topic.

On the displayed page, configure a topic policy in basic mode. The basic mode simply specifies which users or cloud services have permissions to publish messages to the topic. For details, see [Table 8-12](#).

Table 8-12 Description for configuring a topic policy in basic mode

Item	Settings	Description
Users who can publish messages to this topic	Topic creator	Only users under the same account as the topic creator have permissions to publish messages to this topic.

Item	Settings	Description
	All users	All users have permission to publish messages to the topic.
	Specified user accounts	<p>Only specified users have permission to publish messages to the topic.</p> <p>Users are specified in the format urn:csp:iam::domainId:root, in which domainId indicates the account ID of a user. Every two users are separated with a comma (,). SMN does not limit the number of users you can specify, but the total length of a topic policy cannot exceed 30 KB.</p> <p>NOTE</p> <ul style="list-style-type: none">• Enter the account ID of the user and click OK. Other information is automatically supplemented by the system.• To obtain a user's account ID, log in to the SMN console, hover the mouse over the username in the upper right corner, and choose My Credentials from the drop-down list.
Services that can publish messages to this topic	<p>For example, VOD.</p> <p>The services that can publish messages to a topic vary depending on regions.</p>	Selecting VOD grants it permissions for this topic.

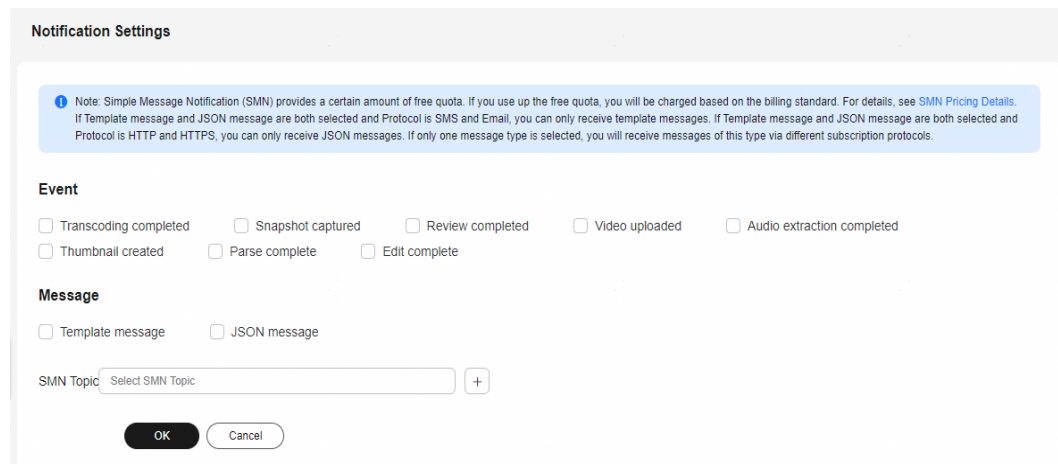
----End

Configuring Notifications

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

Step 2 In the navigation pane, choose **Global Settings > Notification Settings**.

Figure 8-17 Configuring notifications



Step 3 Select one or more events.

NOTICE

If you select both **Snapshot captured** and **Thumbnail created**, only **Snapshot captured** will trigger notifications.

Step 4 Select one or more message types.

NOTE

If **Template message** and **JSON message** are both selected, you will receive template messages via SMS and email, and receive JSON messages via HTTP and HTTPS.

- Select **Template message**. **Table 8-13** describes what a template message looks like. The variables in the notification text message are subject to the actual operation.

Table 8-13 Template message

Event	Status	Message Body
Transcoding completed	Completed	Dear user, your video transcoding task has been completed. Video ID: {asset_id}; name: {title}. Log in to the VOD console or call a VOD API to view transcoding details.
	Failed	Dear user, an error occurred when transcoding your video. Video ID: {asset_id}; name: {title}; error code: {err_code}; error information: {err_msg}.
Snapshot captured	Completed	Dear user, your snapshot task has been completed. Video ID: {asset_id}; name: {title}. Log in to the VOD console or call a VOD API to view snapshot details.

Event	Status	Message Body
	Failed	Dear user, an error occurred when processing your snapshot task. Video ID: {asset_id}; name: {title}; error code: {err_code}; error information: {err_msg}.
Review completed	Completed	Dear user, your review task has been completed. Video ID: {asset_id}; name: {title}; review advice: {suggestion}. Log in to the VOD console or call a VOD API to view review details.
	Failed	Dear user, an error occurred when reviewing your video. Video ID: {asset_id}; name: {title}; error code: {err_code}; error information: {err_msg}.
Video uploaded	Completed	Dear user, your video has been uploaded. Video ID: {asset_id}; name: {title}. Log in to the VOD console or call a VOD API to view video details.
	Failed	Dear user, an error occurred when uploading your video. Video ID: {asset_id}; name: {title}; error code: {err_code}; error information: {err_msg}.
Audio extraction completed	Completed	Dear user, your audio extraction task has been completed. Audio ID: {asset_id}; name: {title}. Log in to the VOD console or call a VOD API to view audio details.
	Failed	Dear user, an error occurred when processing your audio extraction task. Audio ID: {asset_id}; name: {title}; error code: {err_code}; error information: {err_msg}.
Thumbnail created	Completed	Dear user, your video thumbnail has been created. Video ID: {asset_id}; name: {title}. Log in to the VOD console or call a VOD API to view video details.
	Failed	Dear user, your video thumbnail fails to be created. Video ID: {asset_id}; name: {title}; error code: {err_code}; error information: {err_msg}.
Parse complete	Completed	Dear user, your video has been parsed. Video ID: {asset_id}; name: {title}. Log in to the VOD console or call a VOD API to view video details.

Event	Status	Message Body
	Failed	Dear user, an error occurred when parsing your video. Video ID: {asset_id}; name: {title}; error code: {err_code}; error information: {err_msg}.
Edit complete	Completed	Dear user, your editing task has been completed. Video ID: {assetId}; name: {title}. Log in to the VOD console or call a VOD API to view video details.
	Failed	Dear user, an error occurred during the processing of your editing task. Video ID: {assetId}; error code: {err_code}; error information: {err_msg}.

- Select **JSON message**. [Table 8-14](#) describes what a template message looks like.

Table 8-14 JSON message

Parameter	Description	Type
event_type	Event type. The options are as follows: <ul style="list-style-type: none"> – transcodeComplete: transcoding (encryption) completed – thumbnailComplete: snapshot captured – reviewComplete: review completed – createComplete: media file created – audioExtractComplete: audio extracted – coverComplete: thumbnail created – parseComplete: media file parsed – editComplete: media file edited 	String
transcode_info	Transcoding (including encryption) message. For details, see Transcoding Message Body .	TranscodeInfo
thumbnail_info	Snapshot message. For details, see Snapshot Message Body .	ThumbnailInfo
review_info	Review message. For details, see Review Message Body .	ReviewInfo
create_info	Media file upload message. For details, see Media Upload and Audio Extraction Message Body .	AssetInfo
audio_extract_info	Audio extraction message. For details, see Media Upload and Audio Extraction Message Body .	AssetInfo

Parameter	Description	Type
cover_info	Thumbnail message. For details, see Thumbnail Message Body .	CoverInfo
parse_info	Media file parsing completion message. This parameter is available only when a media file has been parsed. For details, see Media Asset Parsing Message Body .	ParseInfo
edit_info	Media file editing completion message. This parameter is available only when a media file has been edited. For details, see Media Asset Editing Message Body .	ParseInfo

Step 5 Select an SMN topic.

Step 6 Click **OK**.

----End

8.8 Workflow Settings

You can create a workflow to transcode a media file and convert its container format, moderate its content, take snapshots, and extract audio. All tasks in the workflow are executed at the same time, accelerating media processing.

Constraints

A workflow orchestrates at least one task. Repeated task orchestration is not allowed.

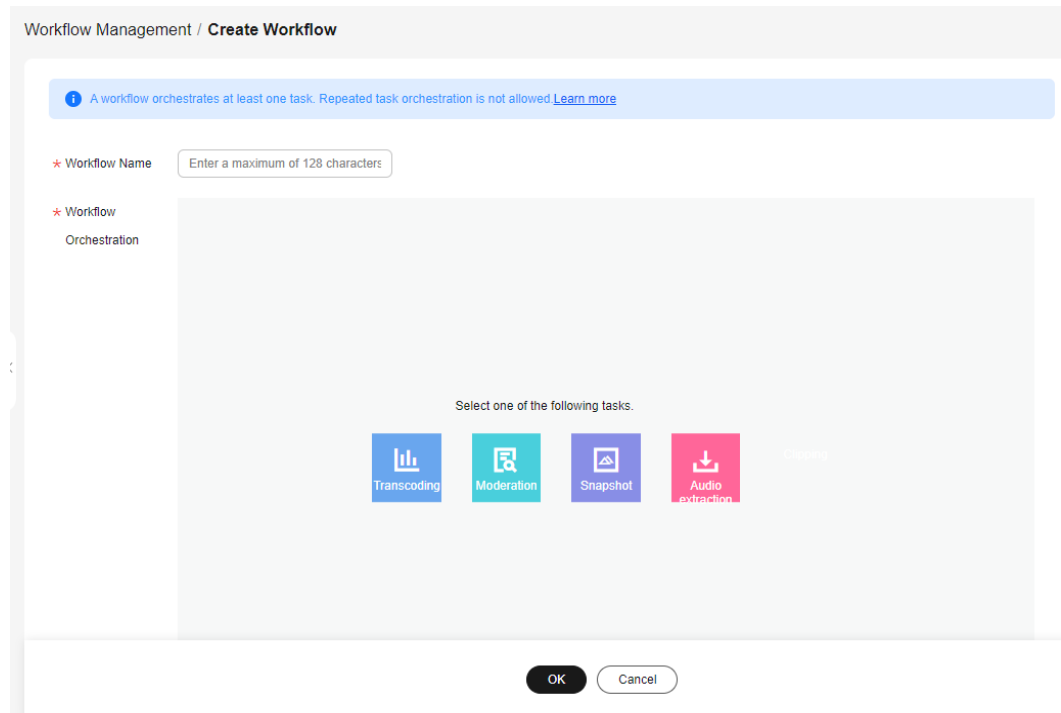
Creating a Workflow

Step 1 Log in to the [VOD console](#).

Step 2 In the navigation pane, choose **Global Settings > Workflows**.

Step 3 Click **Create Workflow**.

Figure 8-18 Creating a workflow



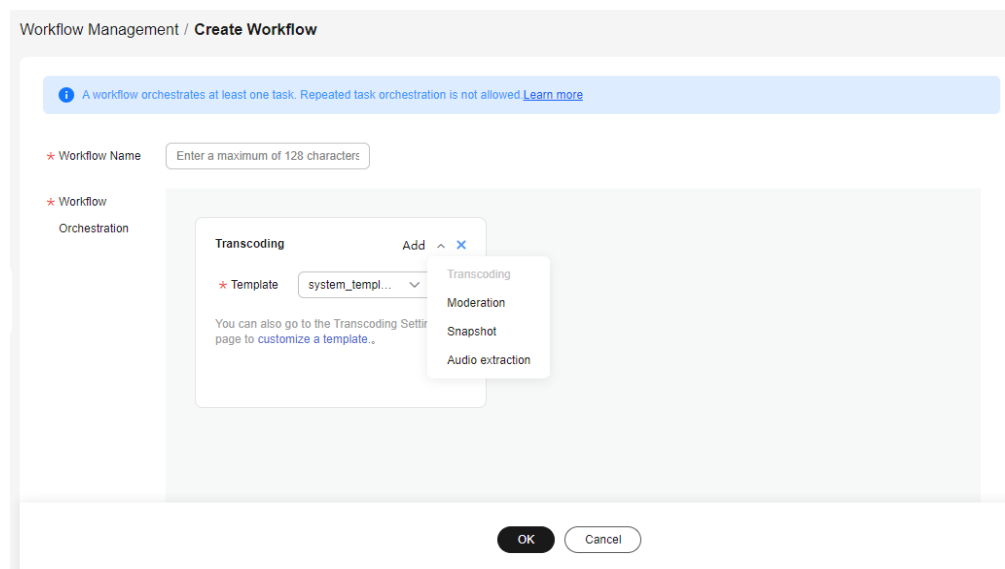
Step 4 Enter a workflow name.

It cannot exceed 128 characters.

Step 5 In the **Workflow Orchestration** area, create a workflow.

1. Select a task.
2. Click **+** in the upper right corner of the selected task to add other tasks. You can also click **x** to delete a task and orchestrate the task again.

Figure 8-19 Orchestration



3. Set task parameters by referring to **Table 1**.

Table 8-15 Task configurations

Task Name	Task Parameters	Description
Transcoding	System template or custom template	If you want to use a custom template group, create a transcoding template first. For details about the restrictions on each transcoding template, see Transcoding Settings .
Mode ration	System template or custom template	For details, see Media Content Review .
Snaps hot	<ul style="list-style-type: none"> - By interval: The system takes snapshots from the first frame of a video based on the configured interval. - At fixed time: The system takes snapshots from a video at configured time points. 	For details, see Snapshot Capturing .
Audio extrac tion	You do not need to set any parameters.	For details, see Audio Extraction .

Step 6 Click **OK**.

The created workflow is displayed in the workflow list.

Step 7 Use the workflow to process the audio/video in [Audio/Video Management](#) and [Audio/Video Upload](#).

----End

9 Review Management (in OBT)

9.1 Enabling Content Moderation Authorization

The **Content Moderation** service of Huawei Cloud has been upgraded. From September 15, 2025, the audio and video moderation capabilities of VOD are updated accordingly. You need to enable the Content Moderation authorization before you can use the audio and video moderation capabilities of VOD.

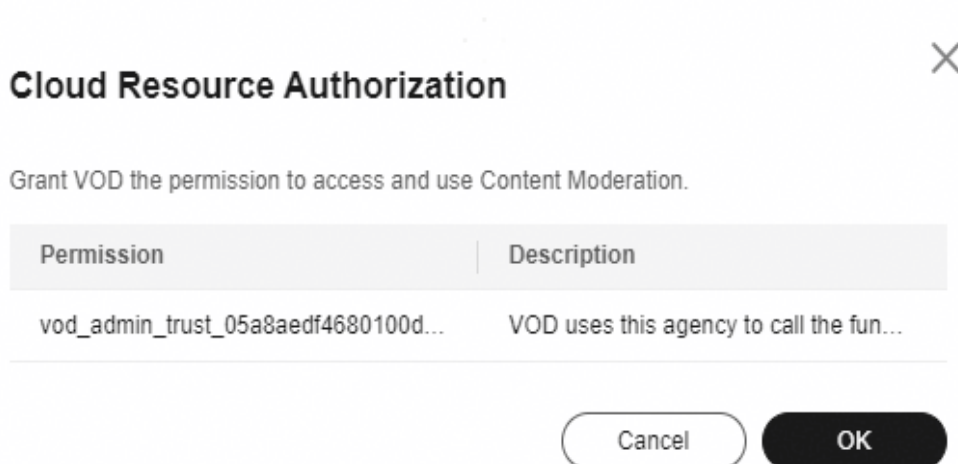
Constraints

IAM users can enable Content Moderation authorization only when they have the permissions below.

Related Cloud Service	Permission
IAM	<ul style="list-style-type: none">• iam:roles:listRoles• iam:roles:createRole• iam:agencies:listAgencies• iam:agencies:createAgency• iam:permissions:checkRoleForAgency• iam:permissions:grantRoleToAgency

Enabling Content Moderation Authorization

- Step 1** Log in to the [VOD console](#).
- Step 2** In the navigation pane, choose **Review Management > Content Moderation**.
- Step 3** In the upper right corner of the page, click **Enable Agency Authorization**, as shown in [Figure 9-1](#).

Figure 9-1 Cloud resource authorization**Step 4** Click **OK**.

The system will create an agency named **vod_admin_trust_{domain-ID}** on the **Agencies** page of the **IAM console**. This assigns VOD the required permissions to access the Content Moderation service and use its functions.

NOTE

Do not delete the agency relationship between VOD and Content Moderation. Otherwise, the audio and video moderation function of VOD will be unavailable.

----End

9.2 Media Content Review

Huawei Cloud VOD provides content review to detect and filter out pornographic, terrorism-related, and politically sensitive information in media files. In doing so, inappropriate media files can be removed in a timely manner to avoid or reduce the adverse impact.

Notes

- Audio and video moderation is not available in the AP-Bangkok region.
- Audio and video moderation is not available for HLS.
- Since October 15, 2025, the audio and video moderation capabilities of VOD have been updated, as a part of the overall upgrade of Content Moderation, a Huawei Cloud EI service. For details, see [Notice on Updates to the VOD Audio and Video Moderation Function](#).
 - To use audio and video moderation, you need to **enable Content Moderation**. The required moderation services vary with the region: text and single-image moderation for CN North-Beijing1; text, single-image, and audio moderation for CN North-Beijing4; and text, single-image, and audio moderation for AP-Singapore.

- Using the audio and video moderation functions of VOD will incur charges from the **Content Moderation** service. For details, see [Content Moderation Billing](#).
- VOD uses only the text, image, and audio moderation capabilities of Content Moderation. You can buy the corresponding packages from Content Moderation.

Review Process

VOD provides two review methods, review after upload and review before upload. Review after upload is available on the VOD console. It means, you upload audio and video and then review the content. If you want to use review before upload, call a VOD API.

Figure 9-2 Review process



- **Intelligent review:** The review module identifies pornographic, terrorism-related, and politically sensitive content in text, thumbnails, and snapshots. By default, this function is enabled.
- **Manual review:** In review details, check the suspected non-compliant media file again. If you confirm the problem, block the media file. Otherwise, approve it.
- **Block:** After you block a media file, its status changes to **Unpublished**. Media files in the **Unpublished** status can only be previewed on the console and cannot be downloaded or played. The streaming URL referenced by Internet is inaccessible.

Prerequisites

- You have enabled the **Content Moderation** service. For details, see [Enabling Content Moderation](#).
- You have authorized VOD to access the Content Moderation service and use its functions. For details, see [Enabling Content Moderation Authorization](#).
- By default, the system template is used for review. If you need to use a custom template, [create a review template](#) and set it as the default template.

Video Content Review

Intelligent review checks the title, description, name, label, category, thumbnail, and content of a video file.

Step 1 Log in to the [VOD console](#).


Step 2 In the navigation pane, choose **Review Management > Content Moderation**.

Step 3 Select a video file and click **Review**. The video review is based on its configured default review template. You can edit the review template on the [Review Settings](#) page.

If the video status changed to **Approved**, **Pending review**, or **Rejected**, intelligent review is complete.

Step 4 Determine whether to start manual review.

You can start manual review in either of the following ways:

- Click  on the left of the video. A maximum of 10 video snapshots are displayed. The system marks non-compliant snapshots. You can re-check the marked snapshots.
- If snapshots are just part of a video and you need to re-check the whole video, click **View Details**.

On the displayed page, snapshots containing pornographic, terrorism-related, or politically sensitive content are marked and texts containing such content are highlighted red. In the preview area, you can play the video for stricter review.

Step 5 Go back to the audio and video list and select multiple video files to approve or block them in batches.

----End

Audio Content Review

Intelligent review checks the title, description, name, label, category, thumbnail, and content of an audio file.

Step 1 Log in to the [VOD console](#).

Step 2 In the navigation pane, choose **Review Management > Content Moderation**.

Step 3 Select an audio file and click **Review**. The audio review is based on its configured default review template. You can edit the review template on the [Review Settings](#) page.

If the audio status changed to **Approved**, **Pending review**, or **Rejected**, intelligent review is complete.

Step 4 Click **View Details** to view review details.

On the displayed page, the thumbnail containing pornographic, terrorism-related, or politically sensitive content is marked and texts containing such content are highlighted red. You can block or approve the audio based on your re-check results.

Step 5 Go back to the audio and video list and select multiple audio files to approve or block them in batches.

----End

9.3 Review Settings

You can review audio and video files for any pornographic, terrorism-related, and politically sensitive content using a system review template or custom template.

Notes

- Confidence levels do not need to be set separately after the content moderation function is updated.

Procedure

Step 1 Log in to the [VOD console](#).

Step 2 In the navigation pane, choose **Review Management > Review Settings**.

Step 3 Click **Custom Template** to open the page for creating a template, as shown in [Figure 9-3](#).

Configure the parameters by referring to [Table 9-1](#).

Figure 9-3 Creating a review template

Table 9-1 Review parameters

Parameter	Description
Template name	A template name can be up to 128 characters long. Only letters, underscores (_), and digits are allowed. Example: MP4_H264
Snapshot Interval	The system automatically takes snapshots based on the interval. Value range: an integer ranging from 1 to 100

Parameter	Description
Obscene content	You can enable one or more moderation options. Confidence levels do not need to be set separately after the content moderation function is updated. If an option is disabled, the corresponding content is not detected.
Terrorism-related content	
Politically sensitive content	

Step 4 Click **OK**.

The new template is displayed in the template list.

Step 5 Click **Set as Default** in the **Template Name** column to set the created template as the default template.

Then the system will review audio and video content based on the settings in the default template.

----End

Editing or Deleting a Custom Template

- After a custom template is created, you can click **Edit** in the template list to modify the template.
- You can also click **Delete** in the template list to delete an unwanted template. If a template is deleted, audio and video using this template will not be deleted.

10 Usage Query

On the VOD console, you can view the traffic and peak bandwidth statistics of CDN, as well as the consumption of storage space and transcoding duration of the VOD origin server. There is a delay of about one hour in usage statistics.

Procedure

- Step 1** Log in to the [VOD console](#).
- Step 2** In the navigation pane, choose **Querying the usage**.
- Step 3** Select **Distribution traffic, Peak Distribution Bandwidth, Media Asset Management, Data retrieval, or Transcode** to view the statistics.

----End

Distribution Traffic

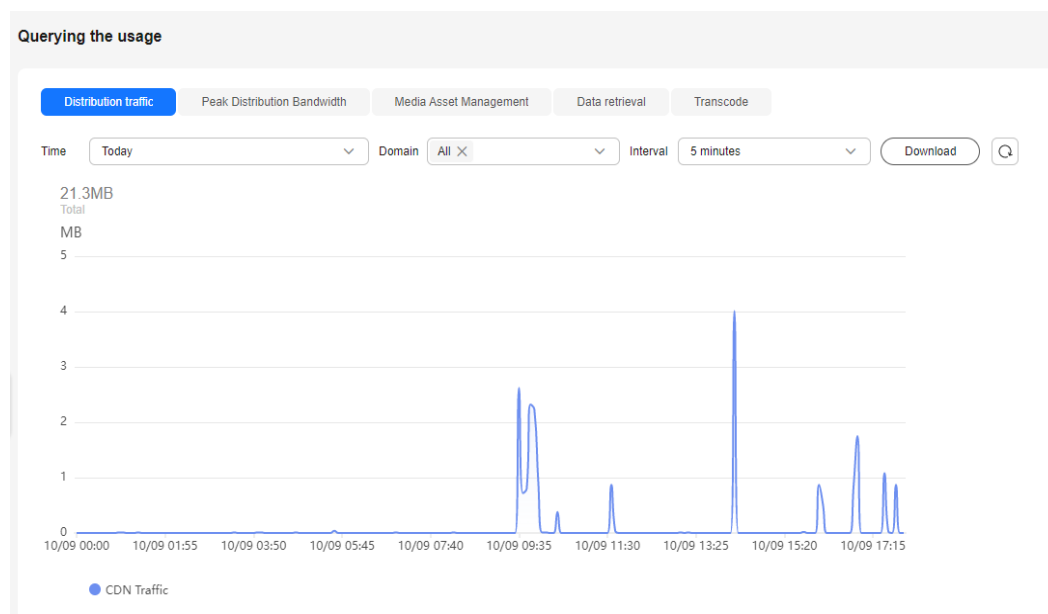
Select the time range, domain name, and time granularity to view CDN traffic statistics.

You can click **Download** to export the CDN traffic statistics to the local PC.

NOTE

- You can query data of the past 90 days.
- The maximum time span of a query is 31 days.
- You can query data of up to 20 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 statistical chart displays the total traffic trend of the selected domain name. You can point to the trend chart and scroll the mouse wheel to zoom in or out on the X-axis within a time range.

Figure 10-1 Total CDN traffic

Peak Distribution Bandwidth

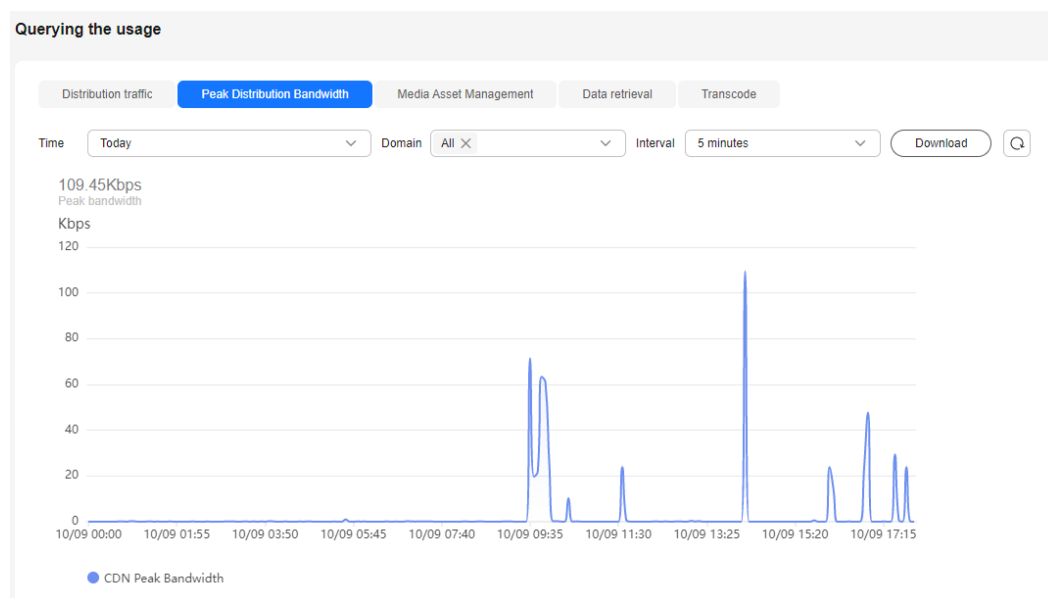
Select the time range, domain name, and time granularity to view CDN peak bandwidth statistics.

You can click **Download** to export the CDN peak bandwidth statistics to the local PC.

NOTE

- You can query data of the past 90 days.
- The maximum time span of a query is 31 days.
- You can query data of up to 20 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 statistical chart displays the peak bandwidth trend of the selected domain name. You can point to the trend chart and scroll the mouse wheel to zoom in or out on the X-axis within a time range.

Figure 10-2 CDN peak bandwidth

Media Asset Management

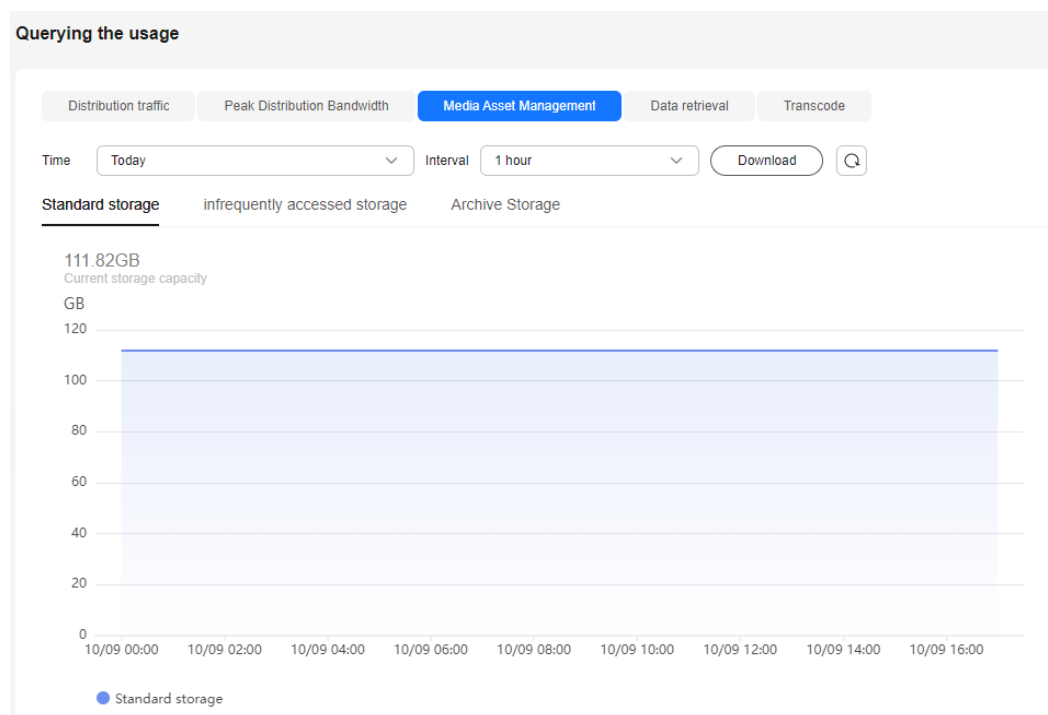
Select the time range and time granularity to view the statistics of standard storage, infrequent access storage, and archive storage of media assets.

You can click **Download** to export the media asset storage statistics to the local PC.

NOTE

- You can query data of the past 30 days.
- The minimum statistical granularity is one hour. For example, data generated from November 6, 2020 08:00:00 (GMT+08:00) to November 6, 2020 09:00:00 (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 statistical chart displays the standard storage volume of the media asset in the selected time range. You can point to the trend chart and scroll the mouse wheel to zoom in or out on the X-axis within a time range.

Figure 10-3 Standard storage statistics

Data Retrieval

Select the time range and time granularity to view the statistics of retrieving media assets of infrequent access storage and archive storage.

You can click **Download** to export the media asset retrieval statistics to the local PC.

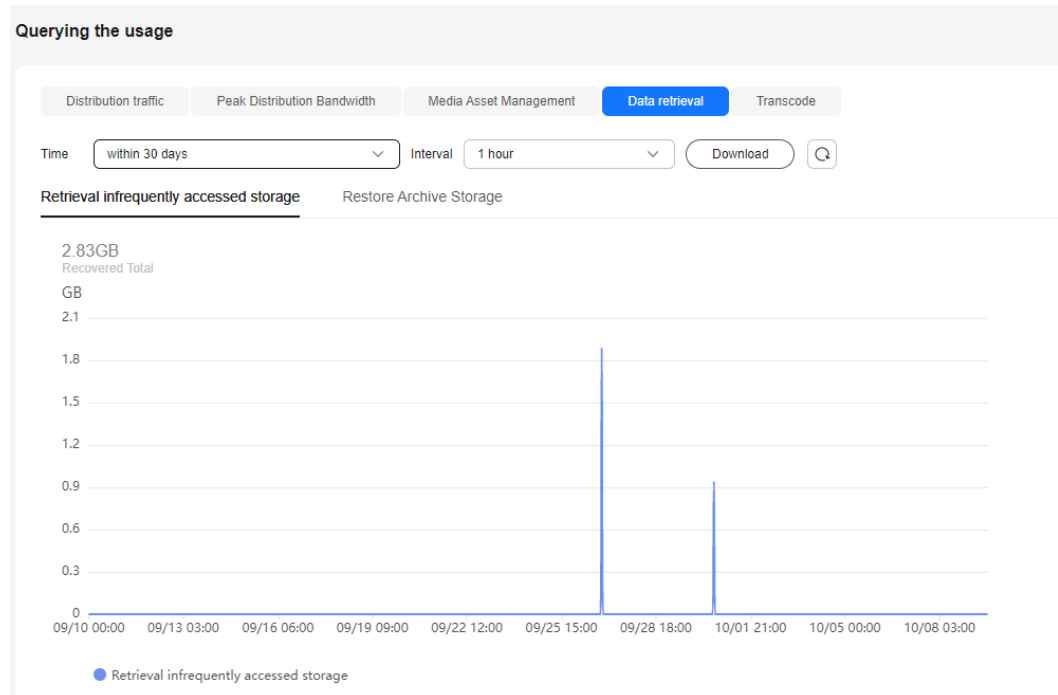
NOTE

- You can query data of the past 30 days.
- The minimum statistical granularity is one hour. For example, data generated from November 6, 2020 08:00:00 (GMT+08:00) to November 6, 2020 09:00:00 (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 statistical chart displays the statistics of the media asset whose storage class changes from infrequent access to standard in the selected time range. You can point to the trend chart and scroll the mouse wheel to zoom in or out on the X-axis within a time range.

If you choose **Restore Archive Storage**, you can view the statistics in the standard and quick retrieval modes.

Figure 10-4 Statistics of the media asset whose storage class changes from infrequent access to standard



Transcoding

Select the time range and time granularity to view the total transcoding duration statistics of a media file.

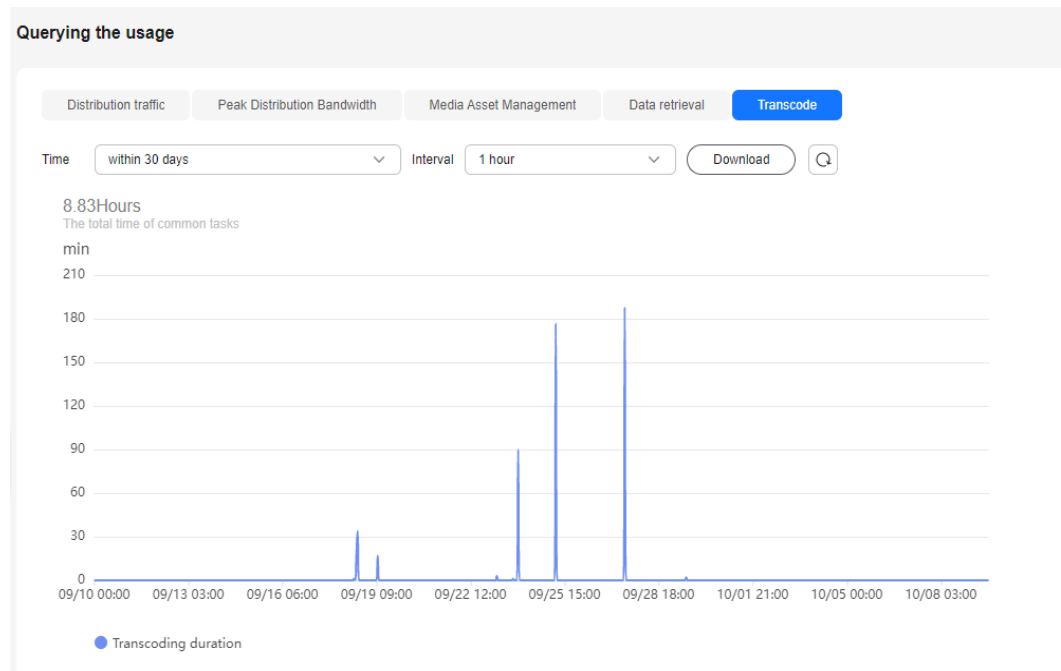
You can click **Download** to export the total transcoding duration statistics of a media file to the local PC.

NOTE

- You can query data of the past 30 days.
- The minimum statistical granularity is one hour. For example, data generated from November 6, 2020 08:00:00 (GMT+08:00) to November 6, 2020 09:00:00 (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 statistical chart displays the total transcoding duration in the selected time range. You can point to the trend chart and scroll the mouse wheel to zoom in or out on the X-axis within a time range.

Figure 10-5 Total transcoding duration



11 Data Analysis

11.1 Distribution Statistics

The distribution statistics function of VOD allows you to query data such as the traffic, bandwidth, and traffic hit ratio on CDN.

About Query

- You can query data of the past 90 days.
- You can query data of up to 20 domain names at a time.
- The maximum time span of a query is 31 days.
- The minimum statistical granularity is five minutes. For example, data generated from April 2, 2019 08:00:00 (GMT+08:00) to April 2, 2019 08:04:59 (GMT+08:00) is displayed at the statistical point April 2, 2019 08:00:00 (GMT+08:00).

Procedure

- Step 1** Log in to the [VOD console](#).
- Step 2** In the navigation pane on the left, choose **Data Analysis > Distribution Statistics**.
- Step 3** Select [Distribution Traffic](#), [Peak Distribution Bandwidth](#), [Requests](#), [Status Codes](#), [Traffic Hit Rate](#), or [Request Hit Rate](#) to view the corresponding statistics.

----End

Distribution Traffic

Select **Time**, **Domain**, **Interval**, and **Transport Protocol** to view CDN traffic statistics within the specified time span, as shown in [Figure 11-1](#).

You can click **IPv4:IPv6 Percentage** on the right to view the volume of CDN traffic and the percentage breakdown for each protocol.


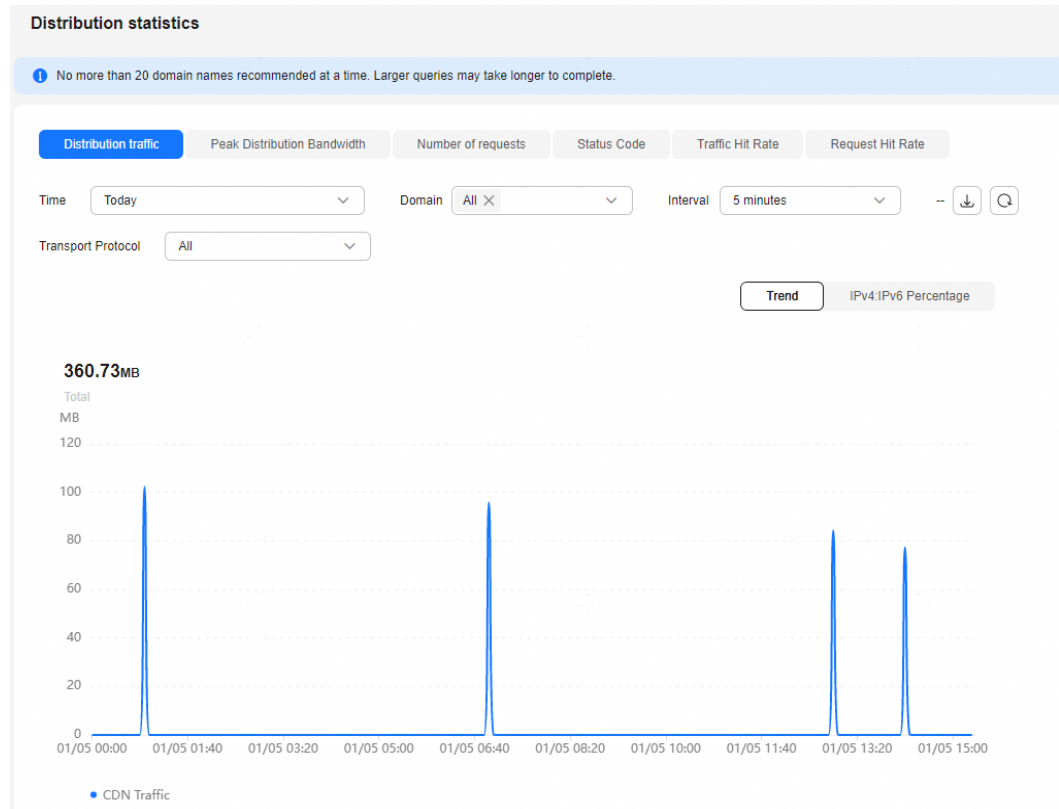
Move the cursor to the trend chart and scroll the mouse wheel to zoom in or zoom out the X axis (time). You can click  to export the statistics details to the local PC.

Figure 11-1 CDN traffic statistics



Peak Distribution Bandwidth

Select **Time**, **Domain**, **Interval**, and **Transport Protocol** to view peak CDN bandwidth statistics within the specified time span, as shown in [Figure 11-2](#).


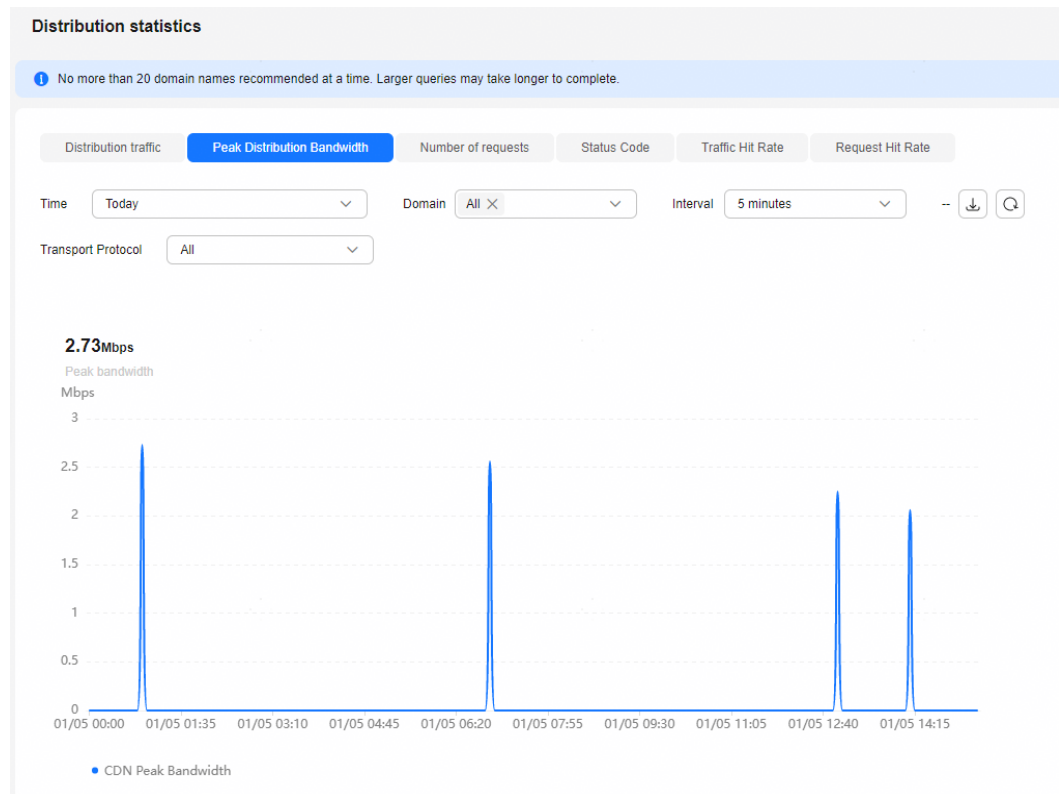
Move the cursor to the trend chart and scroll the mouse wheel to zoom in or zoom out the X axis (time). You can click  to export the statistics details to the local PC.

Figure 11-2 CDN peak bandwidth statistics



Number of Requests

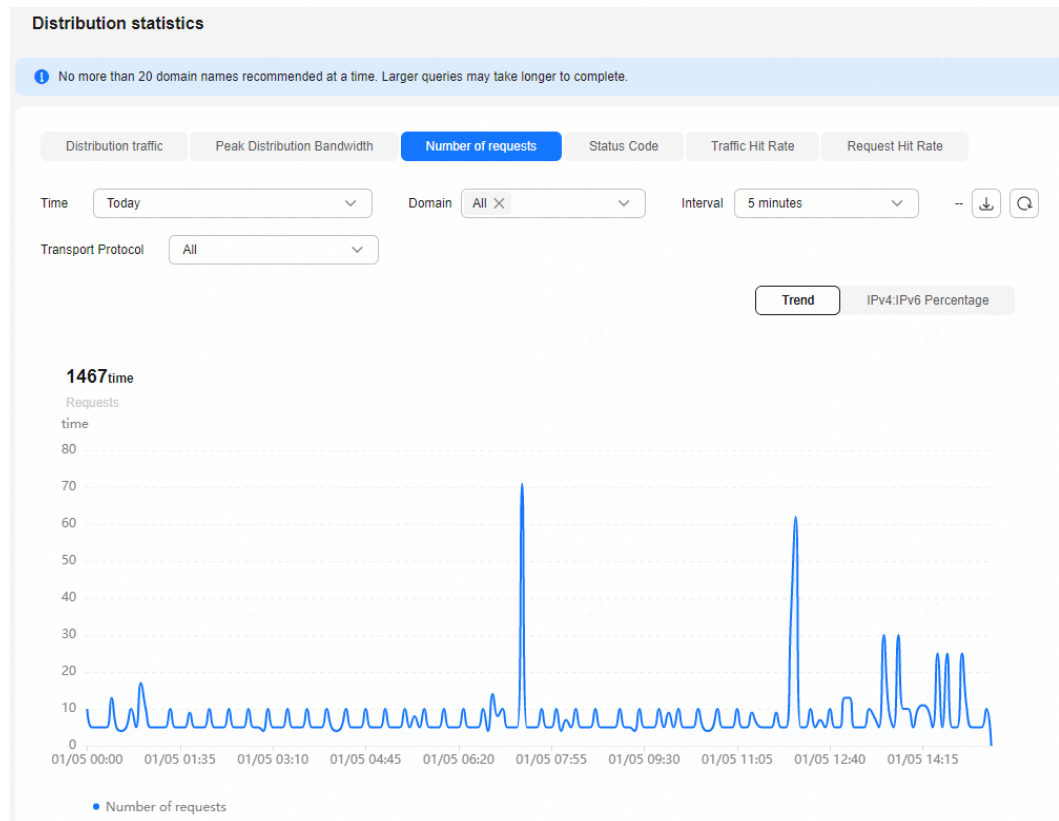
Select **Time**, **Domain**, **Interval**, and **Transport Protocol** to view the number of requests within the specified time span, as shown in [Figure 11-3](#).

You can click **IPv4:IPv6 Percentage** on the right to view the number of requests and the percentage breakdown for each protocol.

Move the cursor to the trend chart and scroll the mouse wheel to zoom in or

zoom out the X axis (time). You can click  to export the statistics details to the local PC.

Figure 11-3 Statistics on the number of requests



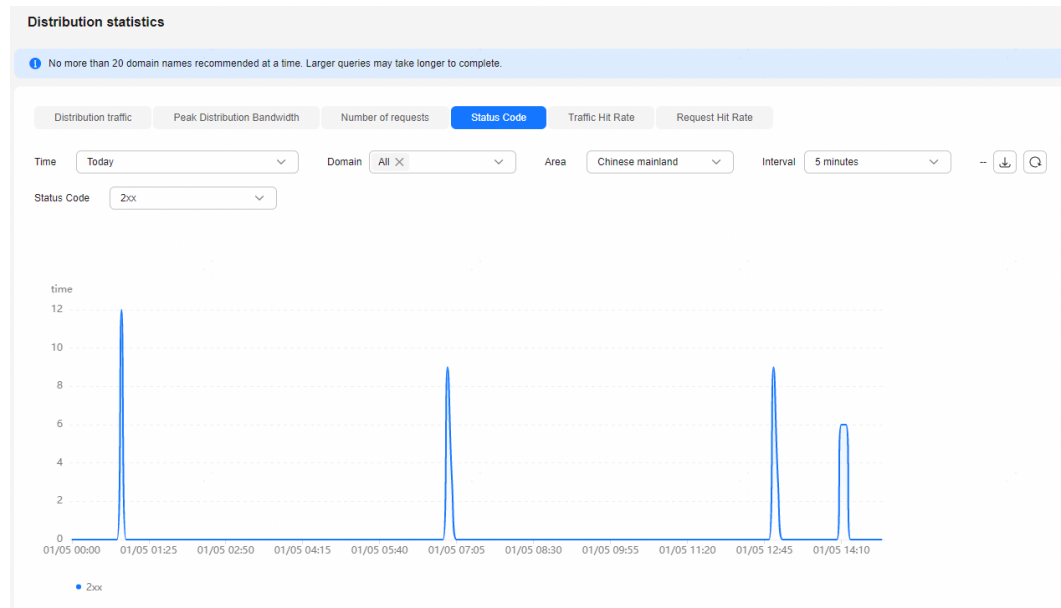
Status Codes

Select **Time**, **Domain**, **Region**, **Interval**, and **Status Code** to view the number of status codes within the specified time span, as shown in [Figure 11-4](#).

Move the cursor to the trend chart and scroll the mouse wheel to zoom in or

zoom out the X axis (time). You can click  to export the statistics details to the local PC.

Figure 11-4 Status code statistics



Traffic Hit Rate

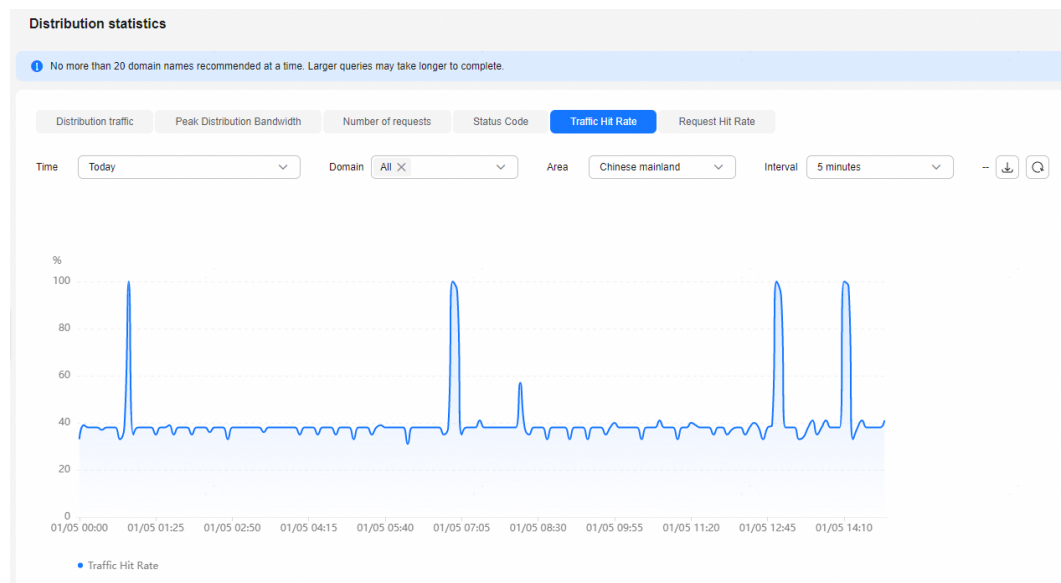
Select **Time**, **Domain**, **Region**, and **Interval** to view traffic hit rate statistics within the specified time span, as shown in [Figure 11-5](#).

Traffic hit rate = Traffic consumed to hit the cache/Total traffic consumed by the requests. The total traffic consumed by the requests equals the traffic consumed to hit the cache plus that consumed for origin pull.

Move the cursor to the trend chart and scroll the mouse wheel to zoom in or

zoom out the X axis (time). You can click  to export the statistics details to the local PC.

Figure 11-5 Traffic hit rate statistics



Request Hit Rate

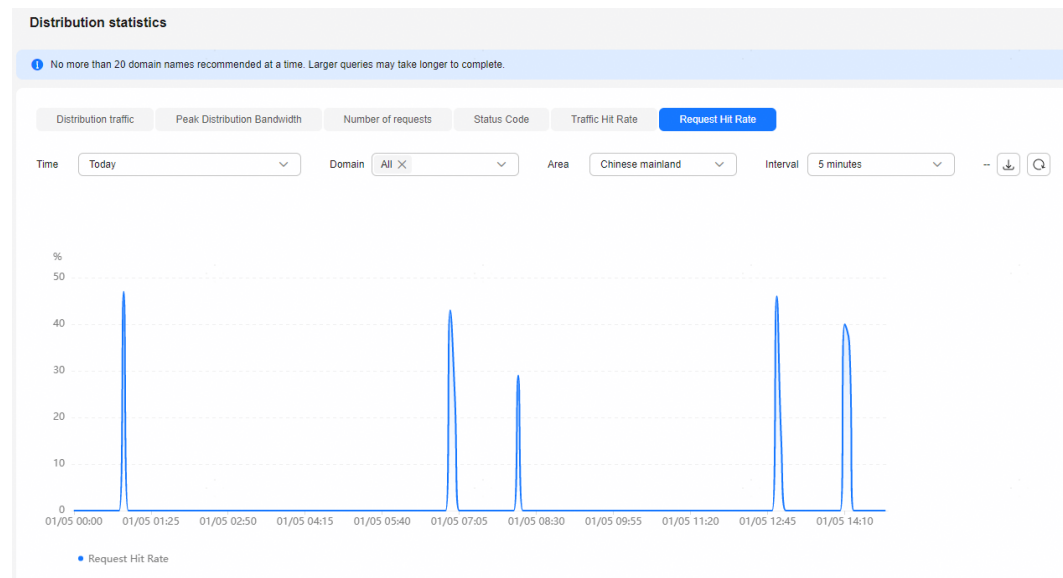
Select **Time**, **Domain**, **Region**, and **Interval** to view request hit rate statistics within the specified time span, as shown in **Figure 11-6**.

Request hit rate = Number of requests that hit the cache/Number of total requests

Move the cursor to the trend chart and scroll the mouse wheel to zoom in or

zoom out the X axis (time). You can click  to export the statistics details to the local PC.

Figure 11-6 Request hit rate statistics



11.2 Playback Statistics

The playback statistics function of VOD allows you to query the number of playback times and ranking (by playback times) of media files by domain name.

Notes

- You can query data about the most requested content of the current day only after 12:00 (Beijing time) of the next day.
- The most requested content is collected based on the number of requests for CDN. The number of requests may be greater than the number of playback times. Therefore, the most requested content may be different from the most played content.
- The following constraints apply to playback statistics:
 - For HLS files, requests for M3U8 files are counted as playbacks, whereas requests for TS segments are not.
 - For other files, such as MP4 files, requests containing a range with a non-zero start value are not counted as playbacks, whereas other requests are.

About Query

- You can query data of the past month from yesterday or earlier.
- You can query the top 100 play time and traffic under all domain names or a single domain name.

Procedure

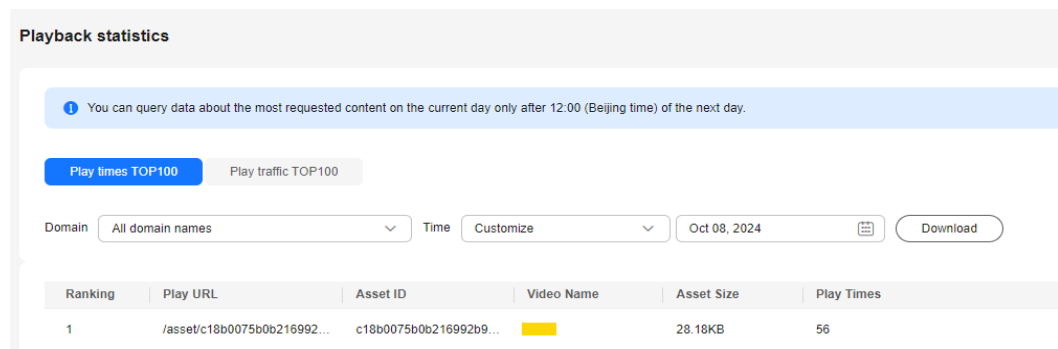
- Step 1** Log in to the [VOD console](#).
- Step 2** In the navigation pane, choose **Data Analysis > Playback Statistics**.
- Step 3** Select **Play times TOP100** or **Play traffic TOP100** to view the statistics.
- End

Top 100 (By Playback Time)

Select **Domain** and **Time** (yesterday or a user-defined period) to view the data of the top 100 audio/video (by playback time).

You can click **Download** to export the statistics details to the local PC.

Figure 11-7 Top 100 (by playback time)

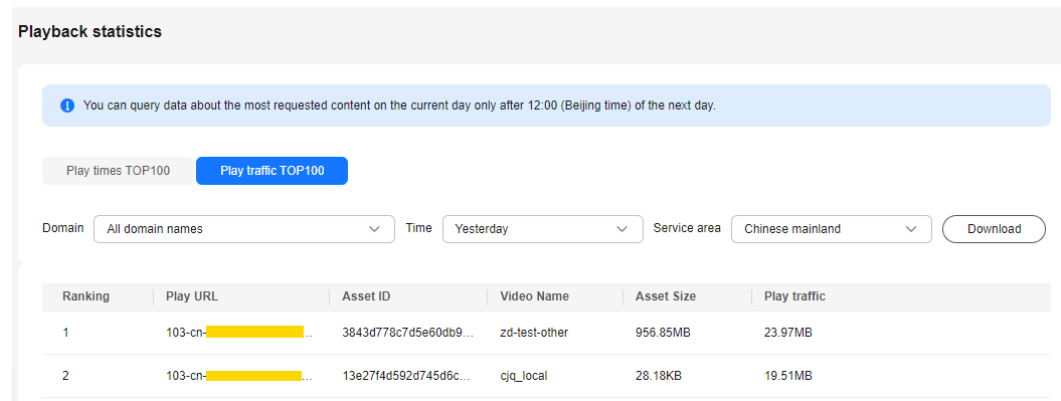


Top 100 (By Playback Traffic)

Select **Domain** and **Time** (yesterday or a user-defined period) to view the data of the top 100 audio/video (by playback traffic).

You can click **Download** to export the statistics details to the local PC.

Figure 11-8 Top 100 (by playback traffic)



12 Task Center

You can view the list of transcoding tasks from the past seven days in the Task Center. You can also query their details.

 **NOTE**

The Task Center will continue to expand its capabilities and support the viewing of more types of tasks.

Prerequisites

You have submitted a transcoding task. For details, see [Transcoding](#).

Procedure

Step 1 Log in to the [VOD console](#).

Step 2 In the navigation pane, choose **Task Center**. The **Task Center** page is displayed, as shown in [Figure 12-1](#).

On the **Task Center** page, you can view the list of transcoding tasks from the past seven days and their details, including the media asset ID, task status, task delivery time, and task end time. You can click **Details** in the **Operation** column of a transcoding task. On the **Task Details** page that is displayed on the right, you can view more information of that task.

Figure 12-1 Task Center

Task Center

The task center currently only supports displaying the list of transcoding tasks and their details for the past 7 days. [Learn More](#)

Select a property or enter a keyword.

Task Type	Asset ID	Task Status	Task delivery time	Task end time	Operation
Transcoding Task	284c4e864f8bf55b69be6c616ddc0f92	Success	Nov 17, 2025 15:19:48	Nov 17, 2025 15:20:23	Details
Transcoding Task	545534d3687197875c08b5583423de02	Failed	Nov 17, 2025 15:19:48	Nov 17, 2025 15:19:52	Details
Transcoding Task	4a9869b0c95e9cb405d93616c090dbf	Success	Nov 17, 2025 15:19:48	Nov 17, 2025 15:20:39	Details
Transcoding Task	0511cb58de560f208b30df674611b089	Success	Nov 17, 2025 15:19:48	Nov 17, 2025 15:20:39	Details
Transcoding Task	16d7b1e2a1b7b1bd4aee39f23a3385f	Success	Nov 17, 2025 15:19:48	Nov 17, 2025 15:20:33	Details
Transcoding Task	187cdf5935eadc5933bce1ab528d2b8	Success	Nov 17, 2025 15:19:48	Nov 17, 2025 15:20:02	Details
Transcoding Task	6f46b9e270dc7de8ba64fbc98e2d069f	Success	Nov 17, 2025 15:19:48	Nov 17, 2025 15:20:38	Details
Transcoding Task	4a1450d74b8402fe70e4b4216838c9ae	Failed	Nov 17, 2025 15:19:48	Nov 17, 2025 15:19:51	Details
Transcoding Task	b42c7989434f9753e8fe71bcc4415607	Failed	Nov 17, 2025 15:19:48	Nov 17, 2025 15:19:51	Details
Transcoding Task	4de6d419890d195acc6415b5bb412c4d	Failed	Nov 17, 2025 15:19:48	Nov 17, 2025 15:19:51	Details

Total Records: 30 +

10 < 1 2 3 ... >

----End

13 Cloud Eye Monitoring

13.1 Monitoring Metrics

This section describes VOD metrics reported to Cloud Eye as well as their namespaces and dimensions. You can use the Cloud Eye console or [APIs](#) to query the VOD metrics and alarms.

You can [view metrics](#) on the management console, [configure alarm rules](#) for metrics, and enable SMN to receive notifications. If a metric meets the alarm condition, Cloud Eye notifies you by SMS message, email, HTTP, or HTTPS.

Namespace

SYS.VOD

Monitoring Metrics

Table 13-1 Supported metrics

ID	Name	Description	Value Range	Unit	Conversion Rule	Dimension	Monitoring Interval (Raw)
flux	Traffic	Total traffic of a domain name in a specified period of time.	≥ 0	bit/s	1024	domain_name	5 minutes

ID	Name	Description	Value Range	Unit	Conversion Rule	Dimension	Monitoring Interval (Raw)
req_num	Access requests	Total number of access requests to a domain name in a specified period of time.	≥ 0	count	-	domain_name	5 minutes
http_code_2xx	Status code summary 2xx	Number of server responses with 2xx status codes for a domain name.	≥ 0	count	-	domain_name	5 minutes
http_code_3xx	Status code summary 3xx	Number of server responses with 3xx status codes for a domain name.	≥ 0	count	-	domain_name	5 minutes
http_code_4xx	Status code summary 4xx	Number of server responses with 4xx status codes for a domain name.	≥ 0	count	-	domain_name	5 minutes
http_code_5xx	Status code summary 5xx	Number of server responses with 5xx status codes for a domain name.	≥ 0	count	-	domain_name	5 minutes

Dimensions

Key	Value
domain_name	VOD domain name You can obtain the value by referring to Querying the Original Dimension Values in Server Monitoring .


13.2 Creating an Alarm Rule

You can configure alarm rules to customize monitored objects and notification policies, so that you can stay informed about domain name statuses.

Prerequisites

To use Cloud Eye to monitor your VOD resources, [submit a service ticket](#).

Procedure

- Step 1** Log in to [Huawei Cloud console](#). Choose **Service List > Management & Governance > Cloud Eye**.
- Step 2** Click  in the upper left corner of the console and select **AP-Singapore** or **CN North-Beijing4**.
- Step 3** In the navigation pane, choose **Alarm Management > Alarm Rules**.
- Step 4** In the upper right corner of the page, click **Create Alarm Rule**.
- Step 5** Configure the parameters as prompted.

For more information, see [Creating an Alarm Rule](#). The key parameters are as follows:

- **Name:** The system generates a random name, and you can change it if needed.
- **Alarm Type:** Select **Metric**.
- **Cloud Product:** Select **VOD - Domain**.
- **Resource Level:** Select **Specific dimension**.
- **Monitoring Scope:** Select **All resources**, **Resource groups**, or **Specific resources**.

- Step 6** Click **Create**.

After the alarm rule is created, the system automatically notifies you when an alarm is triggered.

----End

13.3 Viewing Monitoring Metrics


Cloud Eye monitors the statuses of VOD domain names. You can view VOD metrics on the management console.

Prerequisites

To use Cloud Eye to monitor your VOD resources, [submit a service ticket](#).

Adding a Graph


Add a graph to monitor VOD.

- Step 1** Log in to [Huawei Cloud console](#). Choose **Service List > Management & Governance > Cloud Eye**.
- Step 2** Click  in the upper left corner of the console and select **AP-Singapore** or **CN North-Beijing4**.

- Step 3** In the navigation pane, choose **My Dashboards > Custom Dashboards**.
- Step 4** Click **Create Dashboard** in the upper right corner. The **Create Dashboard** dialog box is displayed.
- Configure the following parameters:
- **Name:** VOD dashboard name, for example, **VOD-Domain**.
 - **Enterprise Project:** Select an enterprise project. The default value is **default**.
- Step 5** Click **OK**. The dashboard details page is displayed.
- Step 6** Choose **Create > Create Graph** and configure graph parameters. For details, see [Adding a Graph](#).
- You can add all VOD monitoring metrics to the same monitoring graph.
- Step 7** Click **Finish**. The graph is added.
- End

Viewing Monitoring Metrics

View the total traffic, total access requests, and status codes of a domain name.

- Step 1** Log in to [Huawei Cloud console](#). Choose **Service List > Management & Governance > Cloud Eye**.
- Step 2** Click  in the upper left corner of the console and select **AP-Singapore** or **CN North-Beijing4**.
- Step 3** In the navigation pane, choose **Cloud Service Monitoring**.
- Step 4** Choose **VOD**. The page of cloud service monitoring details is displayed.
- Step 5** On the **Resources** tab, click **View Metric** in the **Operation** column of the desired domain name.
- You can view the total traffic, total access requests, and status codes of the domain name.
- End

14 Querying Real-Time Traces

14.1 Key Operations Recorded by CTS

VOD has been interconnected with Cloud Trace Service (CTS), which allows you to record operations for future query, audit, and backtracking.

Prerequisites

You have enabled [CTS](#).

Auditable Key Operations

Table 14-1 Operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a media asset	meta	createMeta
Modifying media asset information	meta	updateMeta
Deleting a media asset	meta	deleteMeta
Querying HLS keys	meta	showAssetCipher
Updating a thumbnail (snapshot)	meta	updateCoverByThumbnail
Creating an audio extraction task	meta	createExtractAudioTask
Canceling an audio extraction task	meta	cancelExtractAudioTask
Modifying media asset attributes	meta	updateAssetMeta

Operation	Resource Type	Trace Name
Prefetching media assets on CDN	meta	createAssetPreheatingTask
Replicating media assets from OBS to VOD	meta	publishAssetFromObs
Publishing a media asset	meta	publishAssets
Unpublishing a media asset	meta	unpublishAssets
Confirming media asset upload	meta	confirmAssetUpload
Creating a media asset transcoding task	meta	createAssetProcessTask
Canceling a media asset transcoding task	meta	cancelAssetTranscodeTask
Creating a media asset review task	meta	createAssetReviewTask
Confirming media asset upload (V1.1)	meta	confirmAssetUploadV11
Changing the media asset storage mode	meta	updateStorageMode
Managing subtitles	meta	subtitleModify
Shielding resources	meta	shieldAsset
Setting the URL for obtaining the HLS key	meta	setEncryptConfiguration
Creating a transcoding template	transcodeTemplate	createTranscodeTemplate
Modifying a transcoding template	transcodeTemplate	updateTranscodeTemplate
Deleting a transcoding template	transcodeTemplate	deleteTranscodeTemplate
Creating a media asset category	category	createAssetCategory
Updating a media asset category	category	updateAssetCategory
Deleting a media asset category	category	deleteAssetCategory
Creating a template group set	transcodeTemplate	createTemplateGroupCollection

Operation	Resource Type	Trace Name
Modifying a template group set	transcodeTemplate	updateTemplateGroupCollection
Deleting a template group set	transcodeTemplate	deleteTemplateGroupCollection
Creating a transcoding template group	transcodeTemplate	createTemplateGroup
Modifying a transcoding template group	transcodeTemplate	updateTemplateGroup
Deleting a transcoding template group	transcodeTemplate	deleteTemplateGroup
Creating a URL pull task	pullMetaTask	uploadMetaDataByUrl
Deleting a URL pull task	pullMetaTask	deleteUploadMetaDataByUrlTask
Resuming a URL pull task	pullMetaTask	retrievalUploadMetaDataByUrlTask
Canceling a URL pull task	pullMetaTask	stopUploadMetaDataByUrlTask
Configuring event notifications	message	notifySmnTopicConfig
Creating a review template	review	createReviewTemplate
Modifying a review template	review	updateReviewTemplate
Deleting a review template	review	deleteReviewTemplate
Starting a workflow task	workflow	startWorkflowTask
Creating a workflow	workflow	createWorkflow
Modifying a workflow	workflow	modifyWorkflow
Deleting a workflow	workflow	deleteWorkflow
Creating a watermark template	watermark	createWatermarkTemplate
Modifying a watermark template	watermark	updateWatermarkTemplate
Deleting a watermark template	watermark	deleteWatermarkTemplate
Confirming watermark upload	watermark	confirmImageUpload

Operation	Resource Type	Trace Name
Enabling a watermark	watermark	enableWatermark
Modifying a watermark image	watermark	updateWatermarkImage
Modifying the HTTPS configuration of CDN	domain	modifyDomainHttpsConfig
Creating an acceleration domain name	domain	creatDomain
Setting URL authentication for acceleration domain names	domain	createDomainAuthInfoSetting
Enabling a CDN domain name	domain	enableDomain
Setting referer validation	domain	modifyRefererSetting
Modifying an acceleration domain name	domain	modifyDomain
Disabling an acceleration domain name	domain	disbleDomain
Deleting an acceleration domain name	domain	deleteDomain
Changing the CDN billing mode	bill	updateCdnBill
Enabling VOD	tenant	setTenantInfo
Deleting snapshots of a media asset	thumbnail	deleteAssetThumbnail
Creating an editing task	meta	createAssetEditTask
Canceling an editing task	meta	cancelAssetEditTask
Refreshing CDN cache	meta	createAssetRefreshTask

14.2 Viewing CTS Traces in the Trace List

Scenarios

Cloud Trace Service (CTS) records operations performed on cloud service resources. A record contains information such as the user who performed the operation, IP address, operation content, and returned response message. These records

facilitate security auditing, issue tracking, and resource locating. They also help you plan and use resources, and identify high-risk or non-compliant operations.

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

What Is a Trace?

A trace is an operation log for a cloud service resource, tracked and stored by CTS. Traces record operations such as adding, modifying, or deleting cloud service resources. You can view them to identify who performed operations and when for detailed tracking.

What Is a Management Tracker and Data Tracker?

A management tracker identifies and associates with all your cloud services, recording all user operations. It records management traces, which are operations performed by users on cloud service resources, such as their creation, modification, and deletion.

A data tracker records details of user operations on data in OBS buckets. It records data traces reported by OBS, detailing user operations on data in OBS buckets, including uploads and downloads.

Constraints

- Before the organization function is enabled, you can query the traces of a single account on the CTS console. After the organization function is enabled, you can only view multi-account traces on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled. For details about organization trackers, see [Organization Trackers](#).
- You can only query operation records of the last seven days on the CTS console. They are automatically deleted upon expiration and cannot be manually deleted. To store them for longer than seven days, configure transfer to Object Storage Service (OBS) or Log Tank Service (LTS) so that you can view them in the OBS buckets or LTS log streams.
- After creating, modifying, or deleting a cloud service resource, you can query management traces on the CTS console one minute later and query data traces five minutes later.
- Data traces are not displayed in the trace list of the new version. To view them, you need to go to the old version.
- Data traces cannot be viewed on the CTS console. To view data traces, perform the following steps:

When configuring a data tracker, enable **Transfer to LTS**. This will automatically transfer data traces recorded by CTS to LTS. You can then view audit logs of data traces in an LTS log stream. For details, see [Transferring CTS Traces to LTS and Viewing Them](#).

Prerequisites

1. **Register with Huawei Cloud and complete real-name authentication.**

If you already have a Huawei Cloud account, skip this step. If you do not have one, do as follows:

- a. Log in to the [Huawei Cloud official website](#), and click **Sign Up**.
- b. Sign up for a HUAWEI ID as prompted. For details, see [Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services](#).

Your personal information page is displayed after the registration completes.

- c. Complete [real-name authentication](#) for your individual or enterprise account.


2. **Grant permissions for users.**

If you log in to the console using a Huawei Cloud account, skip this step.

If you log in to the console as an IAM user, first contact your CTS administrator (account owner or a user in the **admin** user group) to obtain the **CTS FullAccess** permissions. For details, see [Assigning Permissions to an IAM User](#).

Viewing Traces in the Trace List of the New Edition

Step 1 Log in to the [CTS console](#).

Step 2 Log in to the management console, click  in the upper left corner, and choose **Management & Deployment > Cloud Trace Service**.

Step 3 In the navigation pane, choose **Trace List**.

Step 4 In the time range drop-down list above the trace list, select a desired query time range: **Last 1 hour**, **Last 1 day**, or **Last 1 week**. You can also specify a custom time range within the last seven days.

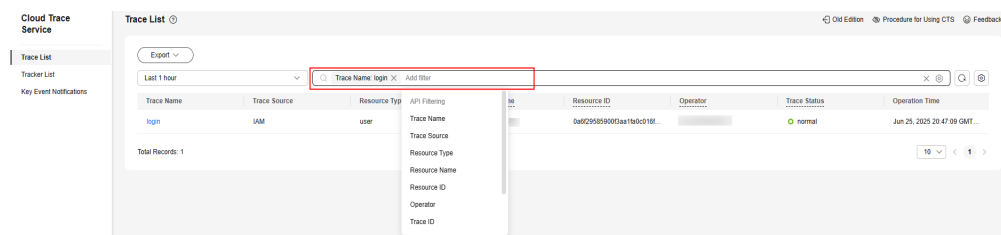
Step 5 The search box above the trace list supports advanced queries. Combine one or more filters to refine your search.

Table 14-2 Trace filtering parameters




Parameter	Description
Read-Only	<p>After selecting the Read-Only filter, you can select either Yes or No from the drop-down list.</p> <ul style="list-style-type: none"> • Yes: filters read-only operation traces, for example, resource query operations. This option is available after Read-Only Trace Reporting has been enabled in the Configuration Center and at least one read-only trace has been triggered. • No: filters non-read-only operation traces, such as creating, modifying, and deleting resources.

Parameter	Description
Trace Name	<p>Name of a trace.</p> <p>The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported.</p> <p>For details about the operations that can be audited for each cloud service, see Supported Services and Operations section "Supported Services and Operations" in the <i>Cloud Trace Service User Guide</i>.</p> <p>Example: updateAlarm</p>
Trace Source	<p>Cloud service name abbreviation.</p> <p>The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported.</p> <p>Example: IAM</p>
Resource Name	<p>Name of a cloud resource involved in a trace.</p> <p>The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported.</p> <p>If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.</p> <p>Example: ecs-name</p>
Resource ID	<p>ID of a cloud resource involved in a trace.</p> <p>The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported.</p> <p>Leave this field empty if the resource has no resource ID or if resource creation failed.</p> <p>Example: <i>{VM ID}</i></p>
Trace ID	<p>Value of the trace_id parameter for a trace reported to CTS.</p> <p>The entered value requires an exact match. Fuzzy matching is not supported.</p> <p>Example: 01d18a1b-56ee-11f0-ac81-*****1e229</p>
Resource Type	<p>Type of a resource involved in a trace.</p> <p>The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported.</p> <p>For details about the resource types of each cloud service, see Supported Services and Operations section "Supported Services and Operations" in the <i>Cloud Trace Service User Guide</i>.</p> <p>Example: user</p>

Parameter	Description
Operator	User who triggers a trace. Select one or more operators from the drop-down list. If the value of trace_type in a trace is SystemAction , the operation is triggered by the service and the trace's operator may be empty. For details about the relationship between IAM identities and operators and the operator username format, see Relationship Between IAM Identities and Operators .
Trace Status	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> ● normal: The operation succeeded. ● warning: The operation failed. ● incident: The operation caused a fault that is more serious than a normal failure, for example, causing other faults.
Enterprise Project ID	ID of the enterprise project to which a resource belongs. To check enterprise project IDs, go to the Enterprise Project Management Service (EPS) console and choose Project Management in the navigation pane. Example: b305ea24-c930-4922-b4b9-*****1eb2
Access Key	Temporary or permanent access key ID. To check access key IDs, hover over your username in the upper right corner of the console and select My Credentials from the pop-up list. On the displayed page, choose Access Keys in the navigation pane. Example: HSTAB47V9V*****TLN9




Step 6 On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.

- Enter any keyword in the search box and press **Enter** to filter desired traces.
- Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
- Click  to view the latest information about traces.
- Click  to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled (), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.

Step 7 (Optional) On the **Trace List** page of the new edition, click **Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

----End

Viewing Traces in the Trace List of the Old Edition

Step 1 Log in to the management console, click  in the upper left corner, and choose **Management & Deployment > Cloud Trace Service**.

Step 2 In the navigation pane, choose **Trace List**.

Step 3 Each time you log in to the CTS console, the new edition is displayed by default. Click **Old Edition** in the upper right corner to switch to the trace list of the old edition.

Step 4 In the upper right corner of the page, select a desired query time range: **Last 1 hour**, **Last 1 day**, or **Last 1 week**. You can also specify a custom time range within the last seven days.

Step 5 Set filters to search for your desired traces.


Table 14-3 Trace filtering parameters


Parameter	Description
Trace Type	Select Management or Data . <ul style="list-style-type: none"> Management traces record operations performed by users on cloud service resources, including creation, modification, and deletion. Data traces are reported by OBS and record operations performed on data in OBS buckets, including uploads and downloads.
Trace Source	Select the name of the cloud service that triggers a trace from the drop-down list.
Resource type	Select the type of the resource involved in a trace from the drop-down list. For details about the resource types of each cloud service, see "Supported Services and Operations" in <i>CTS User Guide</i> .

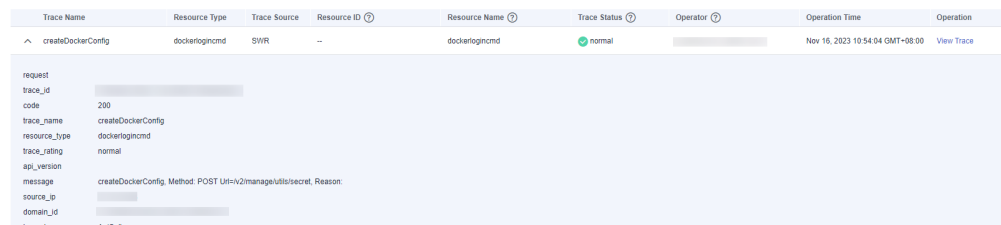
Parameter	Description
Search By	<p>Select one of the following options:</p> <ul style="list-style-type: none"> ● Resource ID: ID of the cloud resource involved in a trace. Leave this field empty if the resource has no resource ID or if resource creation failed. ● Trace name: name of a trace. For details about the operations that can be audited for each cloud service, see "Supported Services and Operations" in <i>CTS User Guide</i>. ● Resource name: name of the cloud resource involved in a trace. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
Operator	<p>User who triggers a trace.</p> <p>Select one or more operators from the drop-down list.</p> <p>If the value of trace_type in a trace is SystemAction, the operation is triggered by the service and the trace's operator may be empty.</p>
Trace Status	<p>Select one of the following options:</p> <ul style="list-style-type: none"> ● Normal: The operation succeeded. ● Warning: The operation failed. ● Incident: The operation caused a fault that is more serious than a normal failure, for example, causing other faults.

Step 6 Click **Query**.

Step 7 On the **Trace List** page, you can also export and refresh the trace list.

- Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.
- Click  to view the latest information about traces.

Step 8 Click  on the left of a trace to expand its details.



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

Step 10 (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

----End

Helpful Links

- For details about the key fields in the trace structure, see [Trace Structure](#) section "Trace References" > "Trace Structure" in the *Cloud Trace Service User Guide* and [Example Traces](#) section "Trace References" > "Example Traces" in the *Cloud Trace Service User Guide*.
- You can use the following examples to learn how to query a specific trace:
 - Use CTS to audit Elastic Volume Service (EVS) creation and deletion operations from the last two weeks. For details, see [Security Auditing](#).
 - Use CTS to locate a fault or creation failure for an Elastic Cloud Server (ECS). For details, see [Fault Locating](#).
 - Use CTS to check all operation records for an ECS. For details, see [Resource Tracking](#).

15 Appendix

15.1 Permissions Management

15.1.1 Creating a User and Granting VOD Permissions

This chapter describes how to use [IAM](#) to implement fine-grained permissions control for your VOD resources. With IAM, you can:

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

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

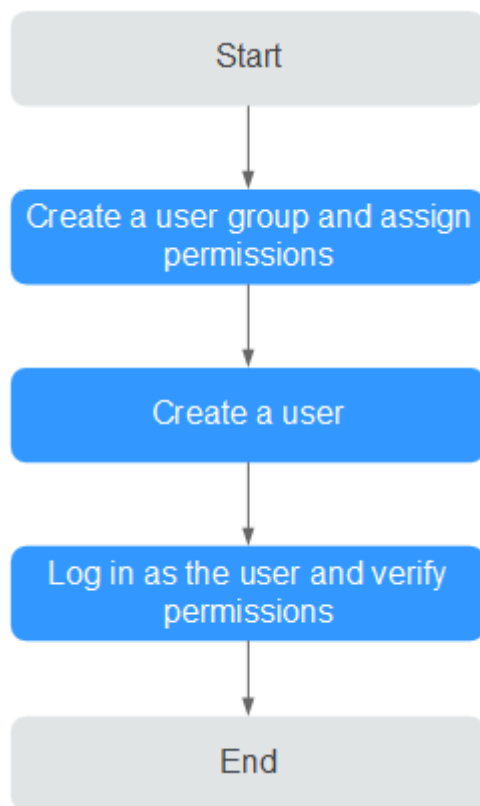
This section describes the procedure for granting permissions (see [Figure 15-1](#)).

Prerequisites

Learn about the permissions (see [Permissions Management](#)) supported by VOD and choose policies or roles according to your requirements.

Process Flow

Figure 15-1 Process of granting VOD read-only permissions



1. **Create a user group and assign permissions** to it.
Create a user group on the IAM console, and attach the **VOD Guest** policy to the group.
2. **Create an IAM user.**
Create a user on the IAM console and add the user to the group created in 1.
3. **Log in** and verify permissions.
Log in to the console by using the user created, and verify that the user only has read permissions for VOD.
 - Choose **Service List > Video on Demand**. The VOD console is displayed. If a message is displayed indicating insufficient permissions for performing the operation, the **VOD Guest** policy has already taken effect.
 - Choose any other service in the **Service List**. If a message appears indicating insufficient permissions to access the service, the **VOD Guest** policy has already taken effect.

Creating a User for Media Isolation

VOD provides nine system policies: VOD Administrator, VOD Operator, VOD Guest, VOD Group Administrator, VOD Group Operator, VOD Group Guest, VOD FullAccess, VOD ReadOnlyAccess, and VOD CommonOperations. For details, see [Permissions Management](#). The VOD Administrator, VOD Operator, and VOD Guest system policies can only be used to assign operation permissions. To isolate

media files stored in VOD, you are advised to use the VOD Group Administrator, VOD Group Operator, and VOD Group Guest system policies, which can also be used to assign operation permissions. Media isolation indicates that only users in the same group can access or manage media created by other users in the group.

Table 15-1 shows an example of media isolation.

Table 15-1 Account permissions

Policy Group	User A (for Management)	User B (for Uploading)	User C (for Watching)
VOD Group Administrator	√	-	-
VOD Group Operator	-	√	-
VOD Group Guest	-	-	√

Regardless of whether an account in the preceding three policy groups is a low-permission or a high-permission one, the account can only operate media created by users in the same group. That is, users A, B, and C can only access media in their own groups.

If user A wants to operate media created by user B, user A must join the VOD Group Operator policy group to which user B belongs.

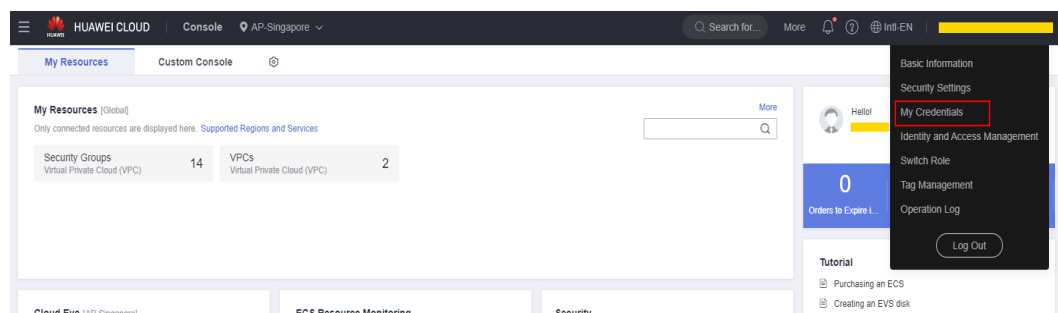
15.2 Obtaining a Project ID

A project ID uniquely identifies a customer.

Procedure

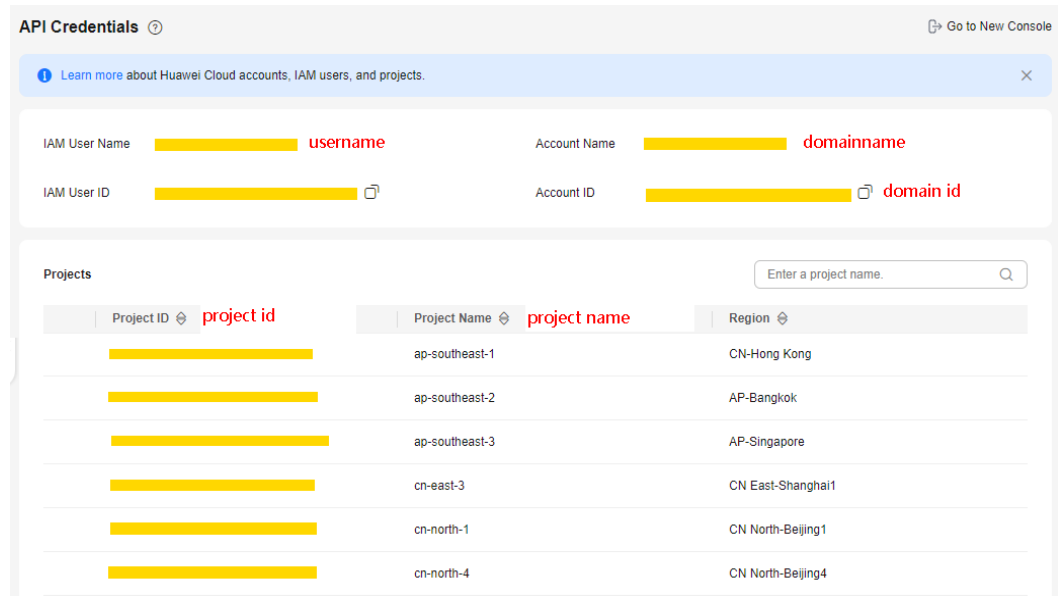
- Step 1** Log in to the [console](#).
- Step 2** Hover over the username in the upper right corner and select **My Credentials** from the drop-down list.

Figure 15-2 Console



- Step 3** On the **API Credentials** page, view project IDs in the project list.

Figure 15-3 Obtaining a project ID



----End

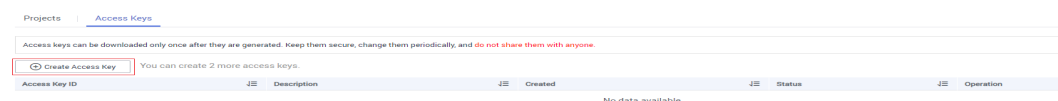
15.3 Obtaining the AK/SK Pair

The access key ID (AK) and secret access key (SK) are a pair of access keys used together to authenticate users who wish to make API requests. The AK/AS pair provides functions similar to a password. If you want to call VOD APIs, the AK/SK pair is required to sign the requests. This ensures the confidentiality and integrity of the requests as well as the correctness of the identities of both parties. Access keys can be generated and managed on the **My Credentials** page.

Procedure

- Step 1** Log in to the [console](#).
- Step 2** Point to the username and choose **My Credentials** from the drop-down list.
- Step 3** In the navigation pane, choose **Access Keys**.
- Step 4** Click **Create Access Key**. On the displayed page, enter the account and password and SMS verification code.

Figure 15-4 Access key



- Step 5** Click **OK** to download the **credentials.csv** file that contains the AK and SK pair.

----End

15.4 JSON Message Body

15.4.1 Transcoding Message Body

Sample Transcoding Success Message

```
{
  "event_type": "transcodeComplete",
  "transcode_info": {
    "asset_id": "14d7b2faba0ddd6b4e8936272d6bc3f",
    "status": "SUCCEED",
    "templateGroupName": "ssw",
    "output": [{
      "play_type": "HLS",
      "url": "https://179.cdn-vod.huaweicloud.com/asset/14d7b2faba0ddd6b4e8936272d6bc3f/
play_video/index.m3u8",
      "encrypted": 0,
      "meta_data": {
        "play_type": 0,
        "codec": "H_264",
        "duration": 0,
        "videoSize": 0,
        "width": 0,
        "hight": 0,
        "bitRate": 0,
        "frameRate": 0
      }
    }, {
      "play_type": "HLS",
      "url": "https://179.cdn-vod.huaweicloud.com/asset/14d7b2faba0ddd6b4e8936272d6bc3f/
play_video/58c6433759c2be34818085006af42d1e_1_1280X720_1500_0.m3u8",
      "encrypted": 0,
      "quality": "HD",
      "meta_data": {
        "play_type": 0,
        "codec": "H_264",
        "duration": 26,
        "videoSize": 3246080,
        "width": 1280,
        "hight": 720,
        "bitRate": 892,
        "frameRate": 1,
        "quality": "HD"
      }
    }
  ]
}
```

Transcoding Message Body Description

Table 15-2 TranscodeInfo structure

Parameter	Description
asset_id	Media ID
status	Event status <ul style="list-style-type: none"> ● SUCCEED: Transcoding succeeded. ● FAILED: Transcoding failed.

Parameter	Description
template_group_name	Transcoding template group name
output	<p>Transcoding output array.</p> <ul style="list-style-type: none"> If outputs are in HLS or DASH format, the number of members in this array is $n+1$, where n indicates the number of transcoding outputs. If outputs are in MP4 format, the number of members in this array is n, where n indicates the number of transcoding outputs. <p>This parameter is used only when status is SUCCEED. For details, see Table 15-3.</p>
error_code	Error code. This parameter is used only when status is FAILED .
error_msg	Error description. This parameter is used only when status is FAILED .

Table 15-3 Output structure

Parameter	Description
play_type	<p>Protocol type</p> <p>The value can be hls, dash, or mp4.</p>
url	Access URL
encrypted	<p>Whether the stream is encrypted</p> <p>The values can be 0 or 1.</p> <ul style="list-style-type: none"> 0: Unencrypted 1: Encrypted
quality	<p>Video quality. The values can be:</p> <ul style="list-style-type: none"> FLUENT SD HD FULL_HD

Parameter	Description
meta_data	<p>Playlist metadata. The values can be:</p> <ul style="list-style-type: none"> ● pack_type: packaging type, such as TS or MP4 ● duration: video duration, in seconds ● size: video size, in bytes ● width: video width (unit: pixel) ● height: video height (unit: pixel) ● bit_rate: average video bitrate ● frame_rate: in FPS

15.4.2 Snapshot Message Body

Sample Frame Capture Success Message

```
{
  "event_type": "thumbnailComplete",
  "thumbnail_info": {
    "asset_id": "14d7b2faba0ddd6b4e8936272d6bc3f",
    "status": "SUCCEED",
    "sample": [{
      "offset": 0,
      "url": "https://179.cdn-vod.huaweicloud.com/asset/14d7b2faba0ddd6b4e8936272d6bc3f/snapshot/sample/0.jpg"
    }, {
      "offset": 5,
      "url": "https://179.cdn-vod.huaweicloud.com/asset/14d7b2faba0ddd6b4e8936272d6bc3f/snapshot/sample/5.jpg"
    }, {
      "offset": 10,
      "url": "https://179.cdn-vod.huaweicloud.com/asset/14d7b2faba0ddd6b4e8936272d6bc3f/snapshot/sample/10.jpg"
    }, {
      "offset": 15,
      "url": "https://179.cdn-vod.huaweicloud.com/asset/14d7b2faba0ddd6b4e8936272d6bc3f/snapshot/sample/15.jpg"
    }, {
      "offset": 20,
      "url": "https://179.cdn-vod.huaweicloud.com/asset/14d7b2faba0ddd6b4e8936272d6bc3f/snapshot/sample/20.jpg"
    }, {
      "offset": 25,
      "url": "https://179.cdn-vod.huaweicloud.com/asset/14d7b2faba0ddd6b4e8936272d6bc3f/snapshot/sample/25.jpg"
    }
  ],
  "dots": []
}
```

Snapshot Message Body Description

Table 15-4 ThumbnailInfo structure

Parameter	Description
asset_id	Media ID
status	Event status <ul style="list-style-type: none"> • SUCCEED • FAILED
sample	Sampling information. This parameter is used only when status is SUCCEED . <ul style="list-style-type: none"> • offset: time offset of a snapshot in the video, in seconds • url: URL for accessing the snapshot
dots	Snapshot information at a specified time point. This parameter is used only when status is SUCCEED . <ul style="list-style-type: none"> • offset: time offset of a snapshot in the video, in seconds • url: URL for accessing the snapshot
error_code	Error code. This parameter is used only when status is FAILED .
error_msg	Error description. This parameter is used only when status is FAILED .

15.4.3 Review Message Body

Sample Review Success Message

```
{
  "event_type": "reviewComplete",
  "review_info": {
    "asset_id": "793636b27b961fb5e35de6580203951b",
    "status": "SUCCEED",
    "suggestion": "BLOCK",
    "text": {
      "suggestion": "PASS"
    },
    "cover": {
      "suggestion": "BLOCK",
      "offset": 0,
      "url": "https://179.cdn-vod.huaweicloud.com/asset/793636b27b961fb5e35de6580203951b/cover/Cover0.jpg",
      "politics": [],
      "terrorism": [
        {
          "confidence": "0.0",
          "label": "bloody"
        },
        {
          "confidence": "0.0",
          "label": "fire"
        },
        {
          "confidence": "0.0",
          "label": "gun"
        },
        {
          "confidence": "0.0",
          "label": "gun"
        }
      ]
    }
  }
}
```

```

        "label": "knife"
    }, {
        "confidence": "0.0",
        "label": "flag"
    }, {
        "confidence": "0.0",
        "label": "symbol"
    }, {
        "confidence": "0.0",
        "label": "dress"
    }, {
        "confidence": "0.9984",
        "label": "crowd"
    }, {
        "confidence": "0.0",
        "label": "tiananmen"
    }, {
        "confidence": "0.0016",
        "label": "normal"
    }
  ]],
  "porn": [{
    "confidence": "0.6997",
    "label": "normal"
  }, {
    "confidence": "0.00040",
    "label": "porn"
  }, {
    "confidence": "0.2999",
    "label": "sexy"
  }
  ]],
  "video": [{
    "suggestion": "BLOCK",
    "offset": 0,
    "url": "https://179.cdn-vod.huaweicloud.com/asset/793636b27b961fb5e35de6580203951b/snapshot/sample0/0.jpg",
    "politics": [],
    "terrorism": [{
      "confidence": "0.0",
      "label": "bloody"
    }, {
      "confidence": "0.0",
      "label": "fire"
    }, {
      "confidence": "0.0",
      "label": "gun"
    }, {
      "confidence": "0.0",
      "label": "knife"
    }, {
      "confidence": "0.0",
      "label": "flag"
    }, {
      "confidence": "0.0",
      "label": "symbol"
    }, {
      "confidence": "0.0",
      "label": "dress"
    }, {
      "confidence": "0.9984",
      "label": "crowd"
    }, {
      "confidence": "0.0",
      "label": "tiananmen"
    }, {
      "confidence": "0.0016",
      "label": "normal"
    }
  ]],
  "porn": [{

```

```

        "confidence": "0.6997",
        "label": "normal"
    }, {
        "confidence": "0.00040",
        "label": "porn"
    }, {
        "confidence": "0.2999",
        "label": "sexy"
    }
  ]
}, {
  "suggestion": "BLOCK",
  "offset": 1,
  "url": "https://179.cdn-vod.huaweicloud.com/asset/793636b27b961fb5e35de6580203951b/
snapshot/sample0/1.jpg",
  "politics": [],
  "terrorism": [{
    "confidence": "0.0",
    "label": "bloody"
  }, {
    "confidence": "0.0",
    "label": "fire"
  }, {
    "confidence": "0.0",
    "label": "gun"
  }, {
    "confidence": "0.0",
    "label": "knife"
  }, {
    "confidence": "0.0",
    "label": "flag"
  }, {
    "confidence": "0.0",
    "label": "symbol"
  }, {
    "confidence": "0.0",
    "label": "dress"
  }, {
    "confidence": "0.9958",
    "label": "crowd"
  }, {
    "confidence": "0.0",
    "label": "tiananmen"
  }, {
    "confidence": "0.0042",
    "label": "normal"
  }
  ],
  "porn": [{
    "confidence": "0.6993",
    "label": "normal"
  }, {
    "confidence": "0.001",
    "label": "porn"
  }, {
    "confidence": "0.2997",
    "label": "sexy"
  }
  ]
}

```

Review Message Body Description

Table 15-5 ReviewInfo structure

Parameter	Description
asset_id	Media ID

Parameter	Description
status	Event status <ul style="list-style-type: none"> • SUCCEED • FAILED
suggestion	Whether the check is passed. block: Sensitive information is detected and the information fails to pass the check. pass: No sensitive information is detected and the information passes the check. review: Manual review is required. When multiple scenarios are detected at the same time, the value of suggestion is subject to the scenario where sensitive information is most likely to be included. That is, if a block occurs in any scenario, the value of suggestion is block . If all scenarios pass the check, the value of suggestion is pass . In addition, if manual review is required in any scenario, the value of suggestion is review . This parameter is used only when status is SUCCEED .
text	Text detection results. This parameter is used only when status is SUCCEED . <ul style="list-style-type: none"> • suggestion: whether the check is passed <ul style="list-style-type: none"> – block: Sensitive information is detected and the information fails to pass the check. – pass: No sensitive information is detected and the information passes the check. – review: Manual review is required. • politics: A list of politically sensitive words are involved. • porn: A list of pornography-related words are involved. • abuse: A list of offensive words are involved.
cover	Thumbnail detection results. This parameter is used only when status is SUCCEED . For details, see Table 15-6 .
video	Video detection results. This parameter is used only when status is SUCCEED . For details, see Table 15-6 .
error_code	Error code. This parameter is used only when status is FAILED .
error_msg	Error description. This parameter is used only when status is FAILED .

Table 15-6 PictureReviewRet structure

Parameter	Notes
suggestion	Whether the check is passed. block: Sensitive information is detected and the information fails to pass the check. pass: No sensitive information is detected and the information passes the check. review: Manual review is required.
url	URL for accessing the snapshot or thumbnail
offset	Time offset of a snapshot in the video, in seconds. This parameter is unavailable for thumbnailing.
politics	Review results of political factors. <ul style="list-style-type: none"> • confidence: The value ranges from 0 to 1. • label: information about the corresponding political figure
terrorism	Review results of terrorism-related content. <ul style="list-style-type: none"> • confidence: The value ranges from 0 to 1. • label: information about terrorism-related content (guns, knives, and fire)
porn	Review results of pornographic content. <ul style="list-style-type: none"> • confidence: The value ranges from 0 to 1. • label: information about pornographic content

15.4.4 Media Upload & Audio Extraction Message Body

Sample Upload Success Message

```
{
  "event_type": "createComplete",
  "create_info": {
    "status": "SUCCEED",
    "title": "Fake video",
    "url": "https://1111116.cdn-vod.huaweicloud.com/asset/81b89afdb5e6c94c68e5028b2747b1f0/3729f0177453c9525b5196d6400f1bb6.flv",
    "asset_id": "81b89afdb5e6c94c68e5028b2747b1f0",
    "user_name": "tmp",
    "meta_data": {
      "play_type": 0,
      "pack_type": "FLV",
      "codec": "UNKNOWN",
      "duration": 0,
      "video_size": 0,
      "width": 0,
      "height": 0,
      "bit_rate": 0,
    }
  }
}
```

```

    "frame_rate": 0
  }
}

```

Sample Extraction Success Message

```

{
  "event_type": "audioExtractComplete",
  "audio_extract_info": {
    "status": "SUCCEED",
    "title": "1080p16m",
    "url": "https://1111116.cdn-vod.huaweicloud.com/asset/d98b70ff435cf417a0a450052be80109/e8f3fd5c82bdb979188ab1a2cb66c08b.mp3",
    "asset_id": "d98b70ff435cf417a0a450052be80109",
    "meta_data": {
      "play_type": 0,
      "pack_type": "MP3",
      "codec": "UNKNOWN",
      "duration": 60,
      "video_size": 0,
      "width": 0,
      "height": 0,
      "bit_rate": 128,
      "frame_rate": 0
    }
  }
}

```

Message Body Description

Table 15-7 AssetInfo structure

Parameter	Description
asset_id	ID of the new media
status	Event status <ul style="list-style-type: none"> SUCCEED FAILED
title	Name of the new media. This parameter is used only when status is SUCCEED .
url	URL for accessing the new media. This parameter is used only when status is SUCCEED .
meta_data	Metadata of the new media. This parameter is used only when status is SUCCEED .
error_code	Error code. This parameter is used only when status is FAILED .
error_msg	Error description. This parameter is used only when status is FAILED .

15.4.5 Thumbnail Generation Message Body

The condition for triggering thumbnail generation is to use the first frame of a video.

Successful Thumbnail Generation (Using the First Frame of a Video)

```
{
  "event_type": "coverComplete",
  "cover_info": {
    "status": "FAILED",
    "title": "XC1",
    "asset_id": "13d570ca574035a3efd7014689c34507",
    "error_code": "VOD.10013",
    "error_msg": "null",
    "cover_type": "HEAD_FRAME_COVER",
    "cover_urls": [{
      "offset": 0,
      "url": "https://651.cdn-vod.huaweicloud.com/asset/10757496f83e0eef6b8593be4eee1175/cover/Cover0.jpg"
    }]
  }
}
```

Message Body Description

Table 15-8 Cover_Info structure

Parameter	Description
status	Event status. <ul style="list-style-type: none"> • SUCCEED: Thumbnail generated. • FAILED: Thumbnail generation failed.
title	Media asset name.
asset_id	Media asset ID.
cover_type	Generated thumbnail type. <ul style="list-style-type: none"> • HEAD_FRAME_COVER: First frame as the thumbnail.
error_code	Error code. This parameter is available only when status is FAILED .
error_msg	Error description. This parameter is available only when status is FAILED .
cover_urls	URL of the thumbnail image. This parameter is available only when the thumbnail is generated.

15.4.6 Media Asset Parsing Message Body

Sample Media Asset Parsing Message

```
{
  "event_type": "parseComplete",
  "parse_info": {
    "status": "SUCCEED",
    "asset_id": "d501e8fd23f550a432f2c528c3823fd8",
    "meta_data": {
      "play_type": 0,
      "pack_type": "MP4",
      "codec": "H.264",
      "audio_codec": "AAC",
      "audio_bit_rate": 126,
      "duration": 53,
      "video_size": 13454959,
      "width": 960,
      "height": 540,
      "bit_rate": 1939,
      "frame_rate": 25,
      "audio_channels": 2,
      "sample": 48000
    },
    "original_url": "https://103.huaweicloud.com/asset/d501e8fd23f550a432f2c528c3823fd8/3cb5b599a92c683c80306f7b4a2dd427.mp4"
  }
}
```

Message Body Description

Table 15-9 ParseInfo structure

Parameter	Description
asset_id	ID of the parsed media asset
status	Event status <ul style="list-style-type: none"> ● SUCCEED: The media asset has been parsed. ● FAILED: The media asset parsing failed.
fileAddr	Address of the OBS bucket where the source media file is. This parameter is used only when the source file is in the tenant bucket.
original_url	URL of the media asset.
meta_data	Media data of the media asset.
error_code	Error code. This parameter is used only when status is FAILED .
error_msg	Error description. This parameter is used only when status is FAILED .

15.4.7 Media Asset Editing Message Body

Sample Media Asset Editing Message

```
{
  "event_type": "editComplete",
  "edit_info": {
    "status": "SUCCEEDED",
    "projectId": "jsgdf87w63grt623r767fs8b2747b1f0",
    "assetId": "81b89afdb5e6c94c68e5028b2747b1f0",
    "taskId": "81b89afdb5e6c94c68e5028b2747b1f0"
  }
}
```

Message Body Description

Table 15-10 ParseInfo structure

Parameter	Description
assetId	ID of the edited media asset.
status	Event status. <ul style="list-style-type: none"> • SUCCEEDED: The media asset has been edited. • FAILED: The media asset editing failed.
projectId	Project ID. For details about how to obtain the project ID, see Obtaining a Project ID .
taskId	ID of the media asset editing task.
error_code	Error code. This parameter is available only when status is FAILED .
error_msg	Error description. This parameter is available only when status is FAILED .

15.5 Installing JDK

This section describes how to install JDK on the Windows and Linux OSs and verify that the installation is successful.

Installing JDK in Windows

- Step 1** Download the JDK file from the [official website](#). JDK 8 is used as an example. Click **DOWNLOAD** below JDK.

Java SE 8u191 / Java SE 8u192

Java SE 8u191 / Java SE 8u192 includes important bug fixes. Oracle strongly recommends that all Java SE 8 users upgrade to this release.

[Learn more](#) ▶

<ul style="list-style-type: none"> ▪ Installation Instructions ▪ Release Notes ▪ Oracle License ▪ Java SE Licensing Information User Manual <ul style="list-style-type: none"> ▪ Includes Third Party Licenses ▪ Certified System Configurations ▪ Readme Files <ul style="list-style-type: none"> ▪ JDK ReadMe ▪ JRE ReadMe 	<p>JDK</p> <p>DOWNLOAD ↓</p>
	<p>Server JRE</p> <p>DOWNLOAD ↓</p>
	<p>JRE</p> <p>DOWNLOAD ↓</p>

Step 2 After the JDK file is downloaded, install the JDK as prompted. For example, install the JDK to the **C:\Program Files\Java\jdk1.8.0_131** directory on the local PC.

Step 3 Configure Java environment variables.

1. Right-click **Computer**, choose **Properties** > **Advanced system settings**.
2. Click the **Advanced** tab, and then click **Environment Variables**.
3. Set JAVA_HOME, PATH, and CLASSPATH (case-insensitive) in the **System variables** area. See [Table 15-11](#).

If the three variables already exist, click **Edit**. If not, click **New**.

Table 15-11 JAVA environment variables

Variable	Value	Description
JAVA_HOME	JDK installation path	Example: C:\Program Files (x86)\Java\jdk1.8.0_1311
PATH	%JAVA_HOME%\bin;%JAVA_HOME%\jre\bin	Add it to the end of the original PATH value.
CLASSPATH	.;%JAVA_HOME%\lib\dt.jar;%JAVA_HOME%\lib\tools.jar;	There is a dot (.) in front of the value.

Step 4 Open the CLI and run **java -version**. The Java environment variables have been configured if the Java version is displayed.

The following is a successful response example:

```
C:\>java -version
java version "1.8.0_131"
Java(TM) SE Runtime Environment (build 1.8.0_131-b11)
Java HotSpot(TM) 64-Bit Server VM (build 25.131-b11, mixed mode)
```

----End

Installing JDK in Linux

Step 1 Download the [JDK installation package](#) based on system requirements. You are advised to download JDK1.8.

Select **Accept License Agreement** before downloading the package.

Figure 15-5 Downloading the JDK

Product / File Description	File Size	Download
Linux ARM 32 Hard Float ABI	72.97 MB	jdk-8u191-linux-arm32-vfp-hflt.tar.gz
Linux ARM 64 Hard Float ABI	69.92 MB	jdk-8u191-linux-arm64-vfp-hflt.tar.gz
Linux x86	170.89 MB	jdk-8u191-linux-i586.rpm
Linux x86	185.69 MB	jdk-8u191-linux-i586.tar.gz
Linux x64	167.99 MB	jdk-8u191-linux-x64.rpm
Linux x64	182.87 MB	jdk-8u191-linux-x64.tar.gz
Mac OS X x64	245.92 MB	jdk-8u191-macosx-x64.dmg
Solaris SPARC 64-bit (SVR4 package)	133.04 MB	jdk-8u191-solaris-sparcv9.tar.Z
Solaris SPARC 64-bit	94.28 MB	jdk-8u191-solaris-sparcv9.tar.gz
Solaris x64 (SVR4 package)	134.04 MB	jdk-8u191-solaris-x64.tar.Z
Solaris x64	92.13 MB	jdk-8u191-solaris-x64.tar.gz
Windows x86	197.34 MB	jdk-8u191-windows-i586.exe
Windows x64	207.22 MB	jdk-8u191-windows-x64.exe

Step 2 Run the following command to decompress the installation package to the JDK directory:

```
tar -xvf jdk-8u191-linux-x64.tar.gz -C /home/vod/jdk/
```

Step 3 Set environment variables.

1. Run the `vi /etc/profile` command to open the **profile** file.
2. Add the following content to the end of the file:

```
#set java environment
export JAVA_HOME=/home/vod/jdk/jdk1.8.0_191
export JRE_HOME=/home/vod/jdk/jdk1.8.0_191/jre
export CLASSPATH=.:$JAVA_HOME/lib/dt.jar:$JRE_HOME/lib/tools.jar
export PATH=$JAVA_HOME/bin:$PATH
```
3. Run the `:wq!` command to save the file and exit.

Step 4 Run the `java -version` command to verify whether JDK has been installed.

If the following JDK version information is displayed, the installation is successful:

```
[root@ecs-c525-web ~]# java -version
java version "1.8.0_191"
Java(TM) SE Runtime Environment (build 1.8.0_191-b11)
Java HotSpot(TM) 64-Bit Server VM (build 25.171-b11, mixed mode)
```

----End