

ApsaraVideo Live

User Guide

User Guide

Console

Function	Description
ApsaraVideo Live CDN domain management	Supports creation and deletion of ApsaraVideo Live CDN domain names.
Live video transcoding setting	Creates different transcoding templates for different AppNames.
Live stream management	Queries real-time live streams and historical live streams.
Live stream blacklist management	Sets and deletes stream blacklists.
Set NotifyUrl	Sets the target URL the live stream information is pushed to.

API

Function	Description
Query online users	<ul style="list-style-type: none">- Gets the number of online users of the RTMP live stream,- Supports query by domain name or stream.
Query streaming blacklist	Gets the blacklist of the currently played live stream under the domain name.
Query stream control history	Gets the operation history of a live stream under a domain name or application.
Query the live stream frame rate and bit rate	<ul style="list-style-type: none">- Gets the frame rate and bit rate history of a live stream,- Supports query by domain name or stream.
Query streaming list	Views the information of all the streams being pushed under a specific domain name (or an application under a specified domain name).
Query streaming history	Views the streaming history of a domain name (or an app under the domain name) within a period of time.
Disable live streaming	Disables the push of a stream. You can set the time to resume the streaming.
Resume live streaming	Resumes the push of a stream.

Set NotifyUrl	Sets the target URL the live stream information is pushed to.
---------------	---

Live video CDN domain

You can create up to 20 live video CDN domains under each account. If you require more than 20 live video CDN domains, open a ticket to contact Alibaba Cloud technical support.

Concurrent live streams

Each live video CDN domain under each account can push up to 20 original (non-transcoded) live streams concurrently. If you enable the transcoding function, each CDN domain can push up to 10 transcoded live streams. If you require more than 20 live video CDN domains, open a ticket to contact Alibaba Cloud technical support.

Streaming

ApsaraVideo Live does not limit the stream bit rate. It supports common resolutions and corresponding bit rates.

We recommend that you set a bit rate not exceeding 4 Mbps to prevent buffering interference.

Domain name management

Add a domain name

Before creating an ApsaraVideo Live activity, you must add an ApsaraVideo Live domain name in the ApsaraVideo Live console.

Prerequisite

If you want to use ApsaraVideo Live service in China, confirm whether your domain name requires ICP record filing. In regions like **China East 2 (Shanghai)** and **China North 2 (Beijing)**, you must complete

the ICP record filing. And in the **Singapore** region, you do not require to complete the ICP record filing. If the record-filing is pending, you must first apply for **Website** record-filing.

Procedure

Log on to the ApsaraVideo Live console.

The console checks the activation status of services on which the product depends. Follow the instructions on the status page.

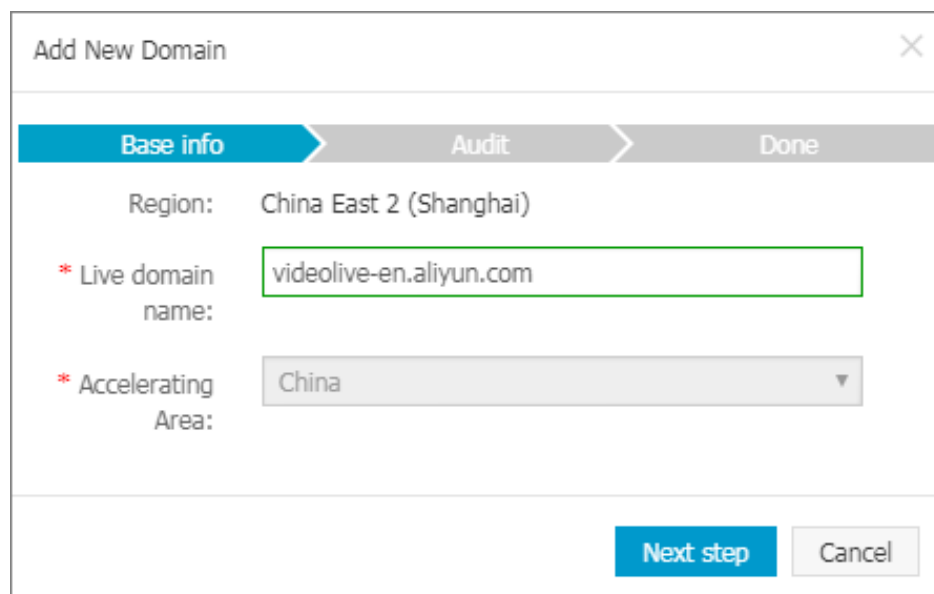
Add a domain name.

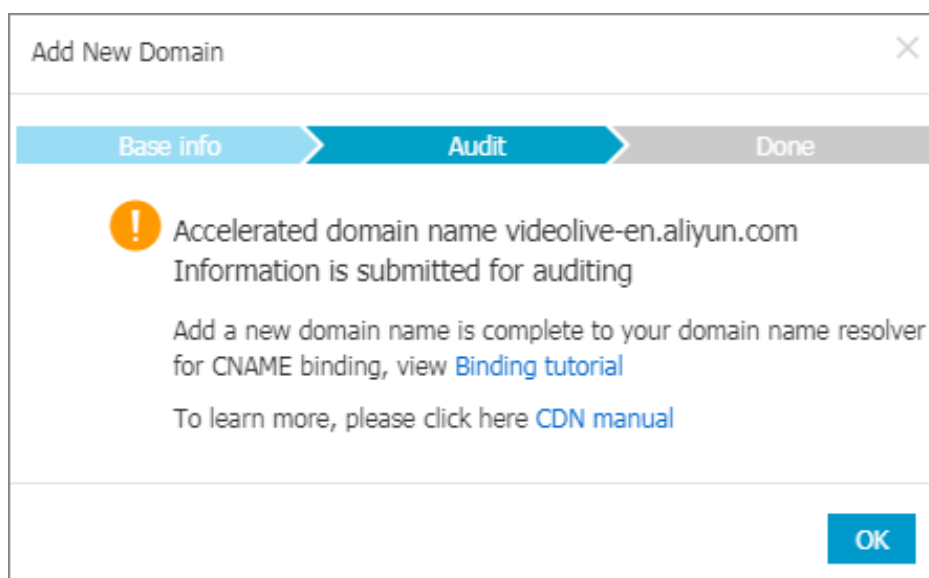
Select the expected region.

Click **Add New Domain**.



Enter the new domain name and click **Next step**.

A screenshot of the 'Add New Domain' dialog box. The dialog has a title bar 'Add New Domain' with a close button (X). Below the title bar is a progress bar with three steps: 'Base info' (active, highlighted in blue), 'Audit', and 'Done'. The 'Base info' section contains three fields: 'Region:' with the value 'China East 2 (Shanghai)', '* Live domain name:' with the value 'videolive-en.aliyun.com' (the input field is highlighted with a green border), and '* Accelerating Area:' with a dropdown menu showing 'China'. At the bottom right of the dialog are two buttons: 'Next step' (highlighted in blue) and 'Cancel'.



After the domain name is successfully configured, the domain name automatically configures the CDN live acceleration function. The live acceleration function is ready to use once the domain name completes CNAME binding.

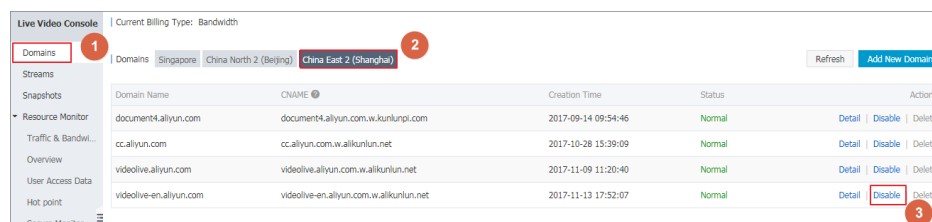
Disable a domain name

Log on to the ApsaraVideo Live console.

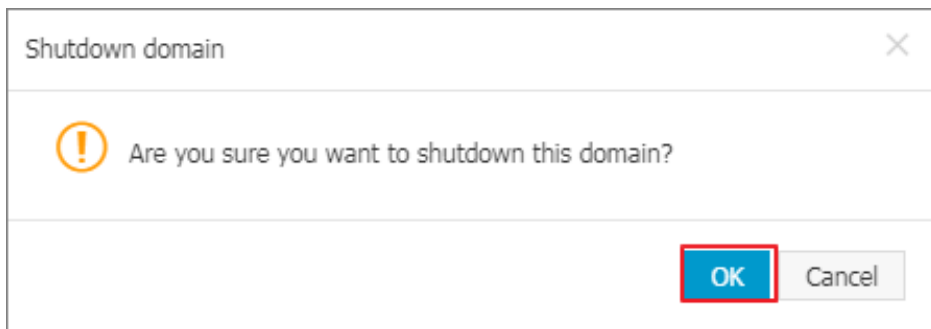
Click **Domains** in the left-side navigation pane.

Select the region in **Domains**.

Select the domain name, and click **Disable** at the right side.



Click **OK**.



The current **Status** of the domain name is **Disabled**.

Live Video Console		Current Billing Type: Bandwidth				
Domains	Domains Singapore China North 2 (Beijing) China East 2 (Shanghai)					Refresh Add New Domain
Streams						
Snapshots						
Resource Monitor						
Traffic & Bandwidth						
Overview						
User Access Data						
Hot point						
Secure Monitor						
		Domain Name	CNAME	Creation Time	Status	Actions
		document4.aliyun.com	document4.aliyun.com.w.kunlunpi.com	2017-09-14 09:54:46	Normal	Detail Disable Delete
		cc.aliyun.com	cc.aliyun.com.w.aliyun.com	2017-10-28 15:39:09	Normal	Detail Disable Delete
		videolive.aliyun.com	videolive.aliyun.com.w.aliyun.com	2017-11-09 11:20:40	Normal	Detail Disable Delete
		videolive-en.aliyun.com	videolive-en.aliyun.com.w.aliyun.com	2017-11-13 17:52:07	Disabled	Detail Enable Delete

Enable a domain name

Log on to the ApsaraVideo Live console.

Click **Domains** in the left-side navigation pane.

Select the region in **Domains**.

Select the domain name, and click **Enable** at the right side.

Live Video Console		Current Billing Type: Bandwidth				
Domains	Domains Singapore China North 2 (Beijing) China East 2 (Shanghai)					Refresh Add New Domain
Streams						
Snapshots						
Resource Monitor						
Traffic & Bandwidth						
Overview						
User Access Data						
Hot point						
Secure Monitor						
		Domain Name	CNAME	Creation Time	Status	Actions
		document4.aliyun.com	document4.aliyun.com.w.kunlunpi.com	2017-09-14 09:54:46	Normal	Detail Disable Delete
		cc.aliyun.com	cc.aliyun.com.w.aliyun.com	2017-10-28 15:39:09	Normal	Detail Disable Delete
		videolive.aliyun.com	videolive.aliyun.com.w.aliyun.com	2017-11-09 11:20:40	Normal	Detail Disable Delete
		videolive-en.aliyun.com	videolive-en.aliyun.com.w.aliyun.com	2017-11-13 17:52:07	Disabled	Detail Enable Delete

Click **OK**.



The current **Status** of the domain name is **Normal**.

Live Video Console		Current Billing Type: Bandwidth				
Domains	Domains					Refresh Add New Domain
Streams	Singapore China North 2 (Beijing) China East 2 (Shanghai)					
Snapshots						
Resource Monitor	Domain Name	CNAME	Creation Time	Status	Actions	
Traffic & Bandwidth	document4.aliyun.com	document4.aliyun.com.w.kunlunpi.com	2017-09-14 09:54:46	Normal	Detail	Disable Delete
Overview	cc.aliyun.com	cc.aliyun.com.w.aliyun.com	2017-10-28 15:39:09	Normal	Detail	Disable Delete
User Access Data	videolive.aliyun.com	videolive.aliyun.com.w.aliyun.com	2017-11-09 11:20:40	Normal	Detail	Disable Delete
Hot point	videolive-en.aliyun.com	videolive-en.aliyun.com.w.aliyun.com	2017-11-13 17:52:07	Normal	Detail	Disable Delete
Secure Monitor						

Delete a domain name

A domain name can only be deleted when its status is **Disabled**.

Procedure

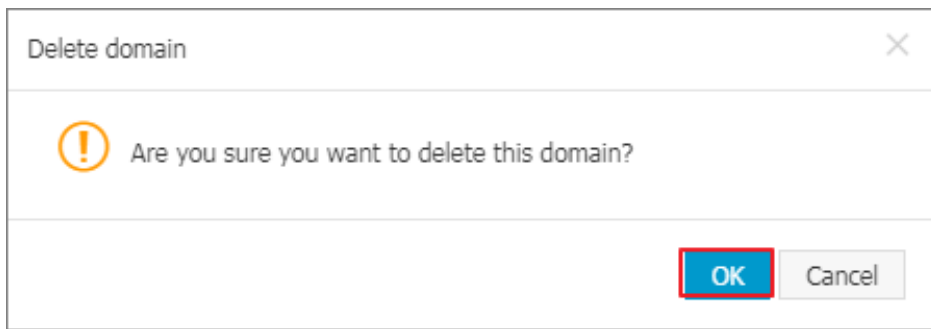
Log on to the ApsaraVideo Live console.

Select the region in **Domains**.

Click **Delete** at the right side of the domain which is disabled.

Live Video Console		Current Billing Type: Bandwidth				
Domains	Domains					Refresh Add New Domain
Streams	Singapore China North 2 (Beijing) China East 2 (Shanghai)					
Snapshots						
Resource Monitor	Domain Name	CNAME	Creation Time	Status	Actions	
Traffic & Bandwidth	videolive-en.aliyun.com	videolive-en.aliyun.com.w.aliyun.com	2017-11-13 17:52:07	Disabled	Detail	Enable Delete
Overview	videolive.aliyun.com	videolive.aliyun.com.w.aliyun.com	2017-11-09 11:20:40	Normal	Detail	Disable Delete
User Access Data	cc.aliyun.com	cc.aliyun.com.w.aliyun.com	2017-10-28 15:39:09	Normal	Detail	Disable Delete
Hot point	document4.aliyun.com	document4.aliyun.com.w.kunlunpi.com	2017-09-14 09:54:46	Normal	Detail	Disable Delete
Secure Monitor						

Click **OK**.

**Note:**

- Follow the procedure, if your domain name is applied for at www.net.cn website.
- If your domain name is not applied for at www.net.cn website, you must transfer your domain name to www.net.cn website and bind CNAME according to the following procedure.

Procedure

Log on to the ApsaraVideo Live console.

Select the region.

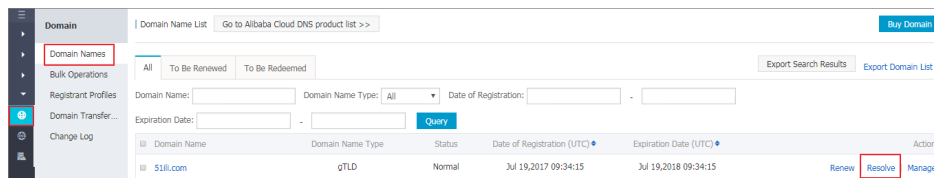
Select the domain name and get the CNAME corresponding to the domain name.

Current Billing Type: Bandwidth					
Domains		Singapore	China North 2 (Beijing)	China East 2 (Shanghai)	
		Refresh		Add New Domain	
Domain Name	CNAME	Creation Time	Status	Actions	
document4.aliyun.com	document4.aliyun.com.w.kunlunpi.com	2017-09-14 09:54:46	Normal	Detail	Disable Delete
cc.aliyun.com	cc.aliyun.com.w.aliyun.com.net	2017-10-28 15:39:09	Normal	Detail	Disable Delete
videolive.aliyun.com	videolive.aliyun.com.w.aliyun.com.net	2017-11-09 11:20:40	Normal	Detail	Disable Delete
videolive-en.aliyun.com	videolive-en.aliyun.com.w.aliyun.com.net	2017-11-13 17:52:07	Normal	Detail	Disable Delete

Log on to the Domain console.

Click **Domain Names**.

Click **Resolve**.



Click **Add Record**.

DNS Settings 51ili.com

DNS Server: vip7.alidns.com, vip8.alidns.com

Search for record: **Add Record**

Type	Host	Line(ISP)	Value	MX Priority	TTL	Status	Actions
<input type="checkbox"/> A	www	Default	114.55.48.61	--	2 minute(s)	--	Edit Disable Delete Remark
<input type="checkbox"/> CNAME	videolive	Default	videolive.aliyun.com.w.alikunlun.net	--	10 minute(s)	--	Edit Disable Delete Remark
<input type="checkbox"/> A	gfdg	China Unicom	11.11.11.11	--	10 minute(s)	--	Edit Disable Delete Remark
<input type="checkbox"/> CNAME	@	Default	ew-2hix8XXX.aliapp.com	--	10 minute(s)	--	Edit Disable Delete Remark
<input type="checkbox"/> CNAME	document4	Default	document4.aliyun.com.w.kunlunpi.com	--	10 minute(s)	--	Edit Disable Delete Remark
<input type="checkbox"/> A	www	Default	120.55.21.95	--	30 minute(s)	--	Edit Disable Delete Remark

Enter the resolution parameters and click **Confirm**.

Add Record

Type: CNAME - Canonical name

Host: videolive-en .51ili.com

ISP Line: Default - Return to the default value when th...

Value: videolive-en.aliyun.com.w.alikunlun.net

TTL: 10 minute(s)

Confirm

Cancel

Select **CNAME-Canonical name** in **Type**.

Enter the secondary domain name of the streaming address in **Host**. For example, if the streaming address is videolive-en.aliyun.com, then the secondary domain name is videolive-en.

Enter the CNAME into **Value** of the domain name list.

- If it is a newly created domain name, the resolution does not require to refresh the DNS.

- Different data is cached on different DNSs. And, if the CNAME changes, it may take up to 48 hours to complete the updates.

Streaming management

A complete live video process includes collection, processing, encoding, packaging, streaming, transmission, transcoding, distribution, decoding, and playing steps. Streaming refers to the process of transmitting live content to the server using streaming tools and other content capturing softwares.

Procedure

Add a domain name.

Log on to the ApsaraVideo Live console.

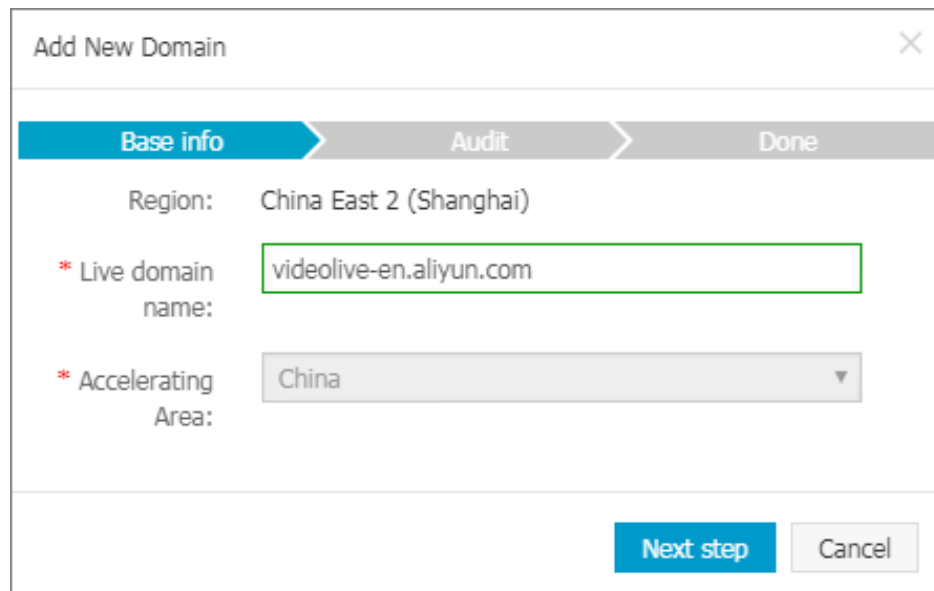
Select the region in **Domains**.

Note: You can select **Singapore**, **China East 2 (Shanghai)** or **China North 2 (Beijing)** in the ApsaraVideo Live console. If you select **China East 2 (Shanghai)** or **China North 2 (Beijing)**, the stream is pushed to the two respectively and undergoes domestic video acceleration. If you select **Singapore**, the stream is pushed to **Singapore** and undergoes foreign video acceleration.

Click **Add New Domain**.



Enter the **Live domain name** and click **Next Step**.



The screenshot shows the 'Add New Domain' dialog box with the 'Base info' tab selected. The 'Region' is set to 'China East 2 (Shanghai)'. The 'Live domain name' field contains 'videolive-en.aliyun.com'. The 'Accelerating Area' dropdown menu is set to 'China'. At the bottom right, there are 'Next step' and 'Cancel' buttons.

Add New Domain

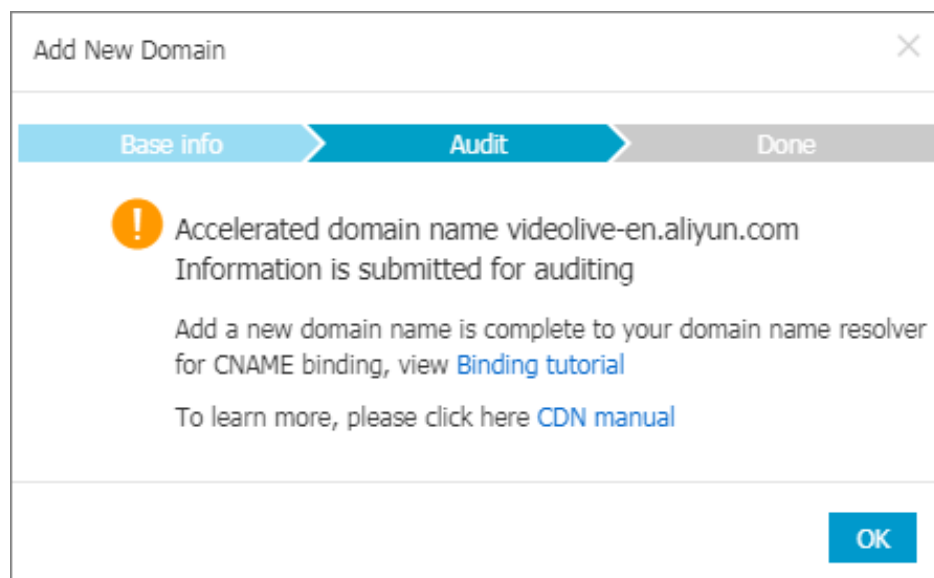
Base info Audit Done

Region: China East 2 (Shanghai)

* Live domain name: videolive-en.aliyun.com

* Accelerating Area: China

Next step Cancel



The screenshot shows the 'Add New Domain' dialog box with the 'Audit' tab selected. A message with an orange exclamation mark icon states: 'Accelerated domain name videolive-en.aliyun.com Information is submitted for auditing'. Below this, it says 'Add a new domain name is complete to your domain name resolver for CNAME binding, view [Binding tutorial](#)'. At the bottom, it says 'To learn more, please click here [CDN manual](#)'. An 'OK' button is at the bottom right.

Add New Domain

Base info Audit Done

! Accelerated domain name videolive-en.aliyun.com Information is submitted for auditing

Add a new domain name is complete to your domain name resolver for CNAME binding, view [Binding tutorial](#)

To learn more, please click here [CDN manual](#)

OK

Get the streaming URL.

Select the region in **Domains**.

Select the domain name and click **Detail** at the right side.

Get **Stream URL** under **Stream Information** in **Base Information** tab.

Streaming operations.

Copy the streaming address to the streaming tool for the push operation. Common streaming test tools are OBS official download, XSplit official download and FMLE official

download.

Note: We recommend that you perform encryption and authentication on the streaming address to reduce the risks such as live video bootlegging or illegal broadcasting without copyright consent. For more information, see [Live video authentication](#).

AppName and StreamName

Live broadcasting address structure

A live video service address consists of three levels of live video management units, that is, the domain name (Domain), an application (AppName) and a live stream (StreamName). You can create multiple apps (AppName) under each domain name (Domain), and multiple live streams (StreamName) under each app.

AppName and StreamName can be edited and customized. Different values generate different streaming and playback addresses.

For example, if an app is named `liveyou` you can create multiple live streams under `live`. The streaming addresses are then as follows:

```
rtmp://video-center.alivecdn.com/{live}/{3}?vhost={live video domain name}
rtmp://video-center.alivecdn.com/{live}/{1}?vhost={live video domain name}
rtmp://video-center.alivecdn.com/{live}/{2}?vhost={live video domain name}
```

You can also create multiple live streams for the app.

```
rtmp://video-center.alivecdn.com/{live1}/{Stream}?vhost={live video domain name}
rtmp://video-center.alivecdn.com/{live2}/{Stream}?vhost={live video domain name}
rtmp://video-center.alivecdn.com/{live3}/{Stream}?vhost={live video domain name}
```

URL authentication function aims to protect the user's website content from the illegal or malicious activity. It is a safe and reliable anti-theft mechanism that protects site resources by coordinating Alibaba Cloud CDN acceleration node with customer resources site. The customer site provides customer with an encrypted URL (including authentication information), which the user then uses to make a request to the acceleration node. The acceleration node verifies the authentication information in the encrypted URL to determine the validity of the request (that is, whether to respond normally to a valid response or refuse an invalid response), thus effectively protecting customer site resources.

Authentication URL composition

Components: Live streaming address/playaddress + verification string, the verification string is caculated according to md5 algorithm by using authentication key + expiration time. This address is applicable to PC end, mobile end, third-party streaming and play tools.

The **Auth KEY** field can be set by the user,

If the **Expire time** in which user visits customer source server exceeds the self-defined time (**timestamp** field designation), the authentication is invalid. For example, if the expire time is 1800s, and the user sets the visit time as 2020-08-15 15:00:00, the link expires at 2020-08-15 15:30:00.

URL authentication concept

Encrypted URL component

```
http://DomainName/Filename?auth_key=timestamp-rand-uid-md5hash
```

Authentication field description

Field	Description
timestamp	expire time, positive integer, fixed length 10, seconds measured from 1970-01-01. Used to control expire time, integer of 10 digit, expire time 1800s.
rand	random number, usually set to 0
uid	not used yet (set to 0)
md5hash	verification string caculated according to md5 algorithm, lowercase letters and digits are supported, fixed length 32

When the server receives the request, it first determines whether the timestamp in the request is shorter than the current time. If it is shorter, then the expire time is thought to be invalid and it returns an HTTP 403 error. If the timestamp is longer than the current time, then a same string is structured (refer to the following composition mode of sstring). The server then calculates the HashValue according to MD5 algorithm, and compares this value with md5hash in the request. If the values are the same, then the authentication is successful; otherwise, it returns an HTTP 403 error.

HashValue is calculated with the following strings,

```
sstring = "URI-Timestamp-rand-uid-PrivateKey" ( URI is the address corresponding to the user's request object,
```

not including parameters , for example : /Filename)
HashValue = md5sum(sstring)

Examples

Pass **req_auth** request object

```
http://cdn.example.com/video/standard/1K.html
```

Set the key to: aliyuncdnexp1234 (set by the user)

The expire time of authentication is 2015-10-10 00:00:00, the seconds calculated is:
1444435200.

The server structures a signature string used to calculate Hashvalue

```
/video/standard/1K.html-1444435200-0-0-aliyuncdnexp1234
```

The server calculates HashValue according to the signature string

```
HashValue = md5sum("/video/standard/1K.html-1444435200-0-0-aliyuncdnexp1234") =  
80cd3862d699b7118eed99103f2a3a4f
```

The URL, when making a request, is

```
http://cdn.example.com/video/standard/1K.html?auth_key=1444435200-0-0-  
80cd3862d699b7118eed99103f2a3a4f
```

The calculated HashValue is consistent with md5hash =
80cd3862d699b7118eed99103f2a3a4f in the user' s request, and the authentication
succeeds.

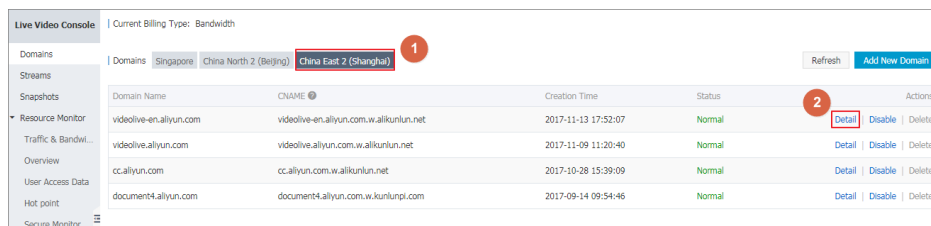
Note: We recommend that the streaming address performs encryption and
authentication operations for enhanced security.

Procedure

Log on to the ApsaraVideo Live console.

Select the region in **Domains**.

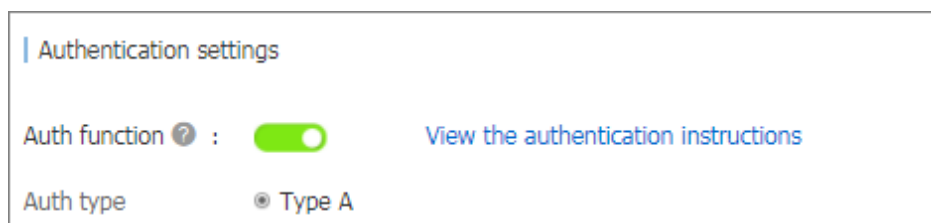
Select the domain name and click **Detail** at the right side.



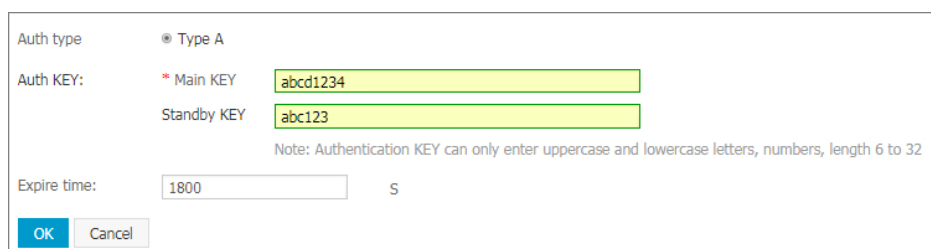
Click **Authenticate**.



Enable **Auth function**.



Enter **Main KEY** and **Standby KEY**, and click **OK**.



Note :

- The main KEY is a key that calculates the encrypted string. It is a mandatory item.
- If the **main KEY** is changed, all the addresses using the **main KEY** instantly becomes invalid. If the **standby KEY** is switched to become the **main KEY**, the streaming or playback address using the **main KEY** does not become invalid instantly, but instead uses the **standby KEY** as a mechanism for performing the switch.

Get the authentication URL.

Enter the stream URL.

You can get the stream URL from the **Base Information** tab.

Note: If you want to define AppName and StreamName, you must replace the AppName and StreamName in the Steam Information with the AppName and StreamName you have defined before before generating the authenticated URL.

Authentication URL Calculator [View the authentication instructions](#)

Stream URL: 1

Auth type: ☐ Type A

Auth KEY: 2

Expire time: s 3

Timestamp: 1510644802

Auth URL: 4

Enter the main KEY and standby KEY in the **Auth KEY** field. It is required for authentication.

Enter the **Expire time** of the authentication URL.

Authentication stands invalid if it exceeds the expire time.

Click **Generate** to get an encrypted auth URL.

Note: The auth URL is configured at the domain name level. If the authentication function under the domain name has taken effect, all the streaming addresses under the domain name must perform the authentication operation. Simultaneously, the play information corresponding to streaming information is also authenticated. We recommend that you use the encrypted address for playing the video.

Function overview

Streaming notification URL or callback URL, is mainly used to call back stream-status real-time information and promptly notify users about the video streaming results.

You can add a callback URL of your background server in the console to Alibaba Cloud, so that when the stream status changes, Alibaba Cloud can send a GET request to your server using the HTTP interface and send the real-time feedback on whether the video streaming succeeds or fails.

Notes

Principle: The real-time stream status feedback is implemented through GET requests sent to the user's server through the HTTP interface. The user server returns 200 responses to the interface. You do not have to identify the URL if normal access is allowed. The following requirements are imposed on the URL responses: In case of access time-out, the URL can be retried. The current time-out duration is 5 seconds, the number of retries is 5, and the interval is 1 second.

It supports the HTTPS address authorized by the certificate authority.

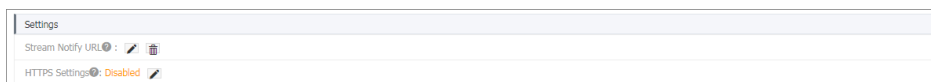
Configuration guide

Log on to the ApsaraVideo Live console.

Select the region in **Domains**.

Select the domain name and click **Detail** at the right side.

Click **Base Information** and set streaming callback address.



Example:

```
https://live.aliyunlive.com/pub? action=publish & app=xc.cdnpe.com & appname=test01 & id=test01 & ip=42.120.74.183 & node=cdnvideocenter010207116011.cm3
```

Configuration in the console is supported, and is optional.

Parameters	Value description
time	Unix timestamp.
usrargs	Streaming parameters.
action	Publish indicates push streaming, and publish_done indicates completion of push

	streaming.
app	The default value is the custom streaming domain name. If no streaming domain name is bound, it is the playback domain name.
appname	Application name.
ID	Stream name.
node	The name of the node or machine in the CDN that receives the stream.
IP	IP address of the client that pushes the stream.

Function overview

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is a security suite of the normal HTTP channel focusing on security. It encapsulates HTTP with the SSL/TLS protocol with SSL/TLS protocol as its security base.

Advantages of HTTPS acceleration

Key user data is encrypted during transmission to prevent sensitive information from the leakage, such as session IDs or cookies that can be maliciously used by attackers.

Data integrity verification is performed during transmission to prevent the hidden danger of man in the middle (MITM) such as DNS or content hijacked or tampered by an unverified third party.

Alibaba Cloud ApsaraVideo Live provides HTTPS secure acceleration schemes. You must enable the secure acceleration mode and then upload the certificate/private key of the CDN domain. The ApsaraVideo Live console also supports viewing, disabling, enabling, and editing the certificates.

If the certificate is configured correctly and enabled, both HTTP access and HTTPS access are supported. If the certificate does not match or is disabled, only HTTP access is supported.

Notes

Configuration restrictions

Feature	Description
Disable and Enable of HTTPS status	Disable: No HTTPS requests are supported and no certificate/private key information is retained. Enable: You must re-upload the certificate/private key to enable the certificate

	again.
View certificate	It allows you to view the certificate only. Viewing private key information is not supported.
Modify and edit certificate	Modification and editing of the certificate are supported, but the effective period for performing these operations is 1 hour. Perform the operation with caution.

Certificate restrictions

The certificate and private key of a CDN domain for which **HTTPS secure acceleration** is enabled, must be uploaded. Both the certificate and private key must be in PEM format.

NOTE: Tengine used in ApsaraVideo Live is based on Nginx, which means certificates that can be read by Nginx are supported (the certificates must be in PEM format).

Only SSL/TLS handshakes containing SNI information is supported.

The certificate and private key that you upload must have a one-to-one correspondence with each other; otherwise, the verification fails.

The effective period of the updated certificate is 1 hour.

Private key with a password is not supported.

Configuration guide

Step 1. Buy a certificate.

To enable **HTTPS secure acceleration**, you must have a certificate that matches the CDN domain. Click **Buy Now** at the Alibaba Cloud Certificates Service to buy a certificate.

Alibaba Cloud Certificates Service

Region : **Asia Pacific SE 2** EU Central 1 Middle East 1

Category : **OV SSL**
OV SSL offers encryption to implement strict identity verification for applicants. It certifies trusted identity.

Select Brand : **Entrust**
Entrust Datacard provides the most stringent organization validation certificate

Type of Domain : **Wildcard Domain** Single Domain Multiple Domain
Protection of one domain name with a wildcard (covering all the domain names at the same level as the "*" wildcard). When you apply for a certificate for a domain name such as *.example.com, the certificate issued will support a.example.com, a1.example.com, a2.example.com and so on, but does not support b.a.example.com, b1.a.example.com and so on

Domains : 1	2	3	4	5	10
20	50	100			

1 Domain(Sans/Subdomain/FQDN/Wildcard)

Current Selected

Region: Asia Pacific SE 2

Category: OV SSL

Select Brand: Entrust

Type of Domain: Wildcard Domain

Domains: 1

Quantity: 1

Duration: 1year(s)

Fee

\$ 1049.00

Buy Now

Quantity : 1

Duration : **1 Year** 2 Years 3 Years

Expired after one year

Step 2. Configure the live video domain name.

Enable HTTPS secure acceleration.

Log on to the ApsaraVideo Live console.

Select the region in **Domains**.

Select the domain name and click **Detail** at the right side.

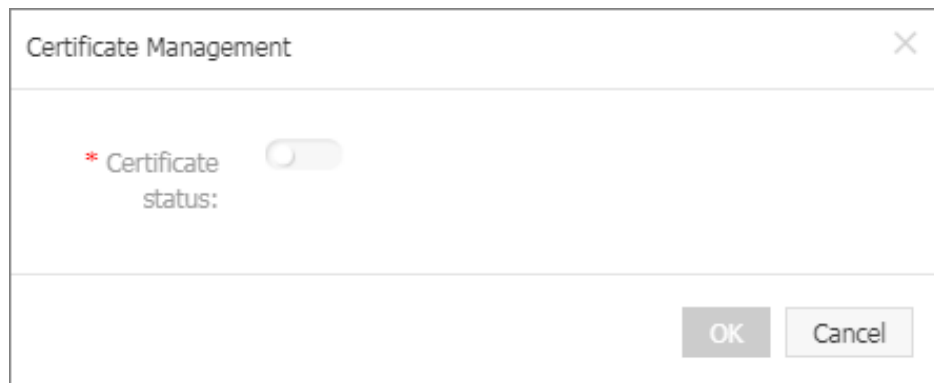
Live Video Console | Current Billing Type: Bandwidth

Domains | Domains | Singapore | China North 2 (Beijing) | **China East 2 (Shanghai)** 1 | Refresh | Add New Domain

Domain Name	CNAME	Creation Time	Status	Actions
videolive-en.aliyun.com	videolive-en.aliyun.com.w.alikunlun.net	2017-11-13 17:52:07	Normal	Detail 2 Disable Delete
videolive.aliyun.com	videolive.aliyun.com.w.alikunlun.net	2017-11-09 11:20:40	Normal	Detail Disable Delete
cc.aliyun.com	cc.aliyun.com.w.alikunlun.net	2017-10-28 15:39:09	Normal	Detail Disable Delete
document4.aliyun.com	document4.aliyun.com.w.kunlunpi.com	2017-09-14 09:54:46	Normal	Detail Disable Delete

Click **Base Information** > **Settings** to perform HTTPS Settings.

Click **HTTPS secure acceleration** to go to the setting page, and then enable **Certificate Status**.



Select a certificate.

Alibaba Cloud ApsaraVideo Live supports two types of certificates for deployment.

Self-owned certificate: You must set the certificate name and then upload the certificate content and private key. The certificate is then saved in the **Alibaba Cloud SSL Certificates console**. You can view it under **My Certificates** tab.

Alibaba Cloud certificate: Certificates purchased from the **Alibaba Cloud Certificates Service** are supported. You can select a certificate name to adapt to the CDN domain.

* Certificate status:

☒

Choose a certificate:

Custom upload ▼

[Purchase certificate](#)

Ali cloud "certificate service" to support the purchase and use of the certificate management and management, [Get to know immediately](#)

* Certificate name

* Certificate content

(Pem encoding)

* Private key:

(Pem encoding)

Jump type:

☒ **Default** ☐ **HTTPS -> HTTP**
☐ **HTTP -> HTTPS**

By default, both HTTPS and HTTP requests are supported

OK

Cancel

NOTE: Only certificates in PEM format are supported.

Set the redirection type.

Forced redirection is supported: The system forces redirection of the users' original

request methods by default.

For example, if **HTTP > HTTPS** redirection is enabled and a user initiates an HTTP request, the server returns a 302 redirect response and the original HTTP request is forcibly redirected to the HTTPS request.

Default: HTTP and HTTPS requests are compatible.

HTTP > HTTPS redirect: Users' HTTP requests are forcibly redirected to the HTTPS requests.

HTTPS > HTTP redirect: Users' HTTPS requests are forcibly redirected to the HTTP requests.

Step 3. Verify whether the certificate has taken effect.

You can access resources by HTTPS when the settings are completed and the certificate are active now. If a green HTTPS mark appears in your browser, it indicates that currently a private connection is established with the website and HTTPS secure acceleration is effective.



Procedure

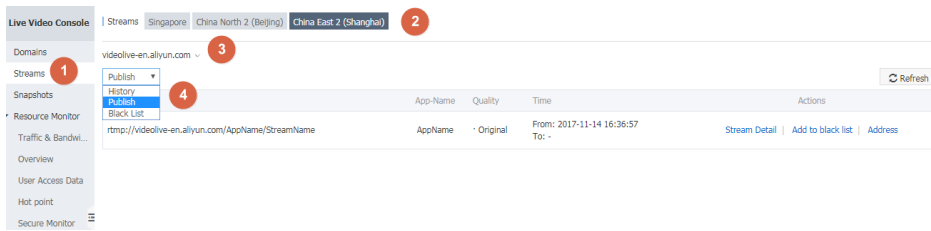
Log on to the ApsaraVideo Live console.

Click **Streams** in the left-side navigation pane.

Select the region.

Select the domain name.

You can then select **History**, **Publish** or **Black List** based on your needs to check the streams information under different statuses.



In a live video environment, buffering interference often leaves a biggest impact on the live video streaming. The general cause is poor bandwidth stability of the uplink transmission.

The ApsaraVideo Live console monitors the uplink traffic. This can easily view the uplink transmission status of the live stream to check if there is any problem.

View the monitoring data

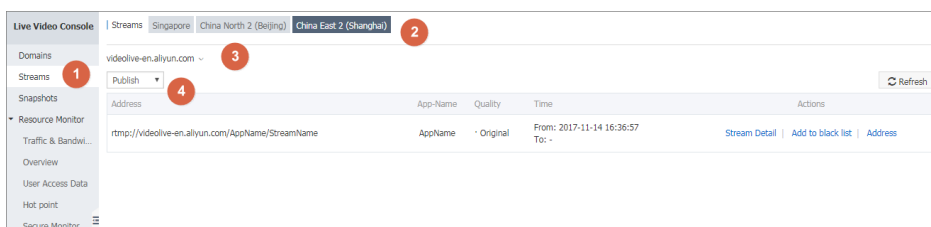
Log on to the ApsaraVideo Live console.

Click **Streams** in the left-side navigation pane.

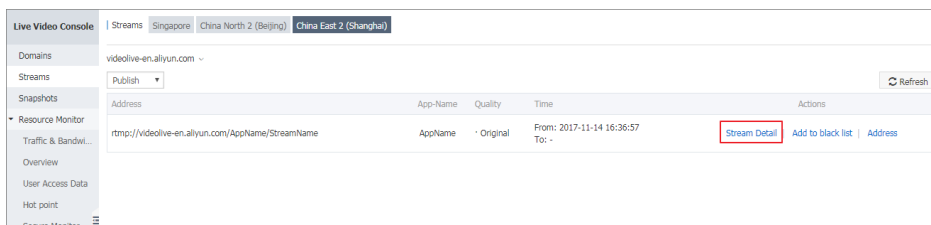
Select the region.

Select the domain name.

Select the stream status.



Select the streaming address and click **Stream Detail** at the right side.

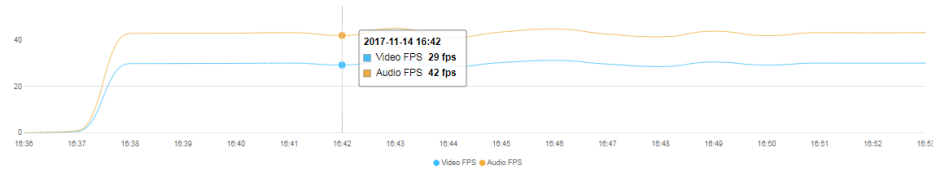


View the stream data such as Publish info, Video FPS, Audio FPS and Bit Rate.

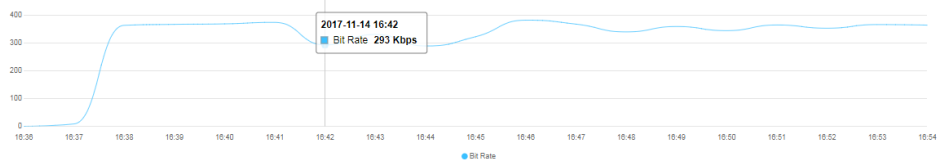
Publish Info

Stream Detail		
Publish Info		
Stream URL: <code>rtmp://videolive-en.aliyun.com/AppName/StreamName</code>		
Domain: <code>videolive-en.aliyun.com</code>	AppName: <code>AppName</code>	StreamName: <code>StreamName</code>
Time duration: 00:20:03	AVG Bit Rate: 323.44 Kbps	AVG FPS: 27.91 fps [video] 40.09 fps [audio]

Frame rate



Bit rate



On an average, the stream data is updated every minute. When the data status appears to be smooth, the valley and the peak values are comparatively stable. This indicates that the uplink transmission is comparatively stable too. If sharp fluctuations occur, we recommend you check the stability of the uplink transmission.

Causes of choppy streaming

Several factors can cause video playback to buffer incorrectly. The following recommendations are troubleshooting tips that may help resolve streaming issues:

Mobile phone configuration.

Streaming consumes CPU resources. During the streaming process, low-end mobile phones with poor hardware configuration may encounter poor quality video if the overall CPU usage exceeds 80%. This affects the video collection and viewing experience on the user terminals.

Video collection parameter settings.

A video must have at least 15 frames per second (FPS) or higher to make sure smooth playback. An FPS set lower than this rate may result in unstable video quality. Note that if the frame rate is set for more than 30 FPS, the image content may not be viewed naturally by most of the viewers. Additionally, a higher frame rate also increases the bandwidth cost of

the video transmission.

Network bandwidth.

Common network factors include:

Network bandwidth size

Confirm the bandwidth size provided by the network operator and whether the bandwidth is sufficient for this live video transmission.

Downlink bandwidth usage

Check whether any data downloading activity occupies the network bandwidth.

System resource usage

Check whether a large number of programs are running in the background, and terminate any unnecessary programs to save the resources.

After the streaming address is added to the blacklist, the streaming operations under this domain name, and any operations thereafter, are suspended. To continue the streaming operations, you must restore the address from the blacklist.

Procedure

Log on to the ApsaraVideo Live console.

Click **Streams** in the left-side navigation pane.

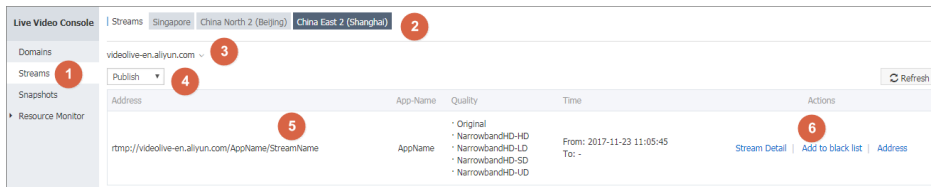
Select the region.

Select the domain name.

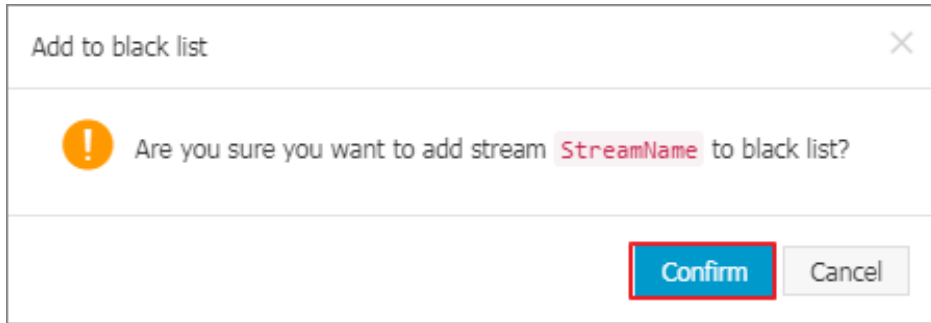
Select the status of the stream.

Select the address.

Click **Add to blacklist** from the Actions column, from the selected address.



Click **Confirm**.



The address is added to the blacklist successfully.

Do as follows to restore the address from the blacklist.

Log on to the ApsaraVideo Live console.

Click **Streams** in the left-side navigation pane.

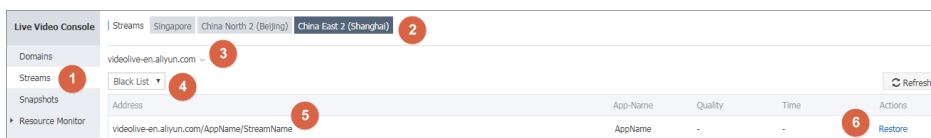
Select the region.

Select the domain name.

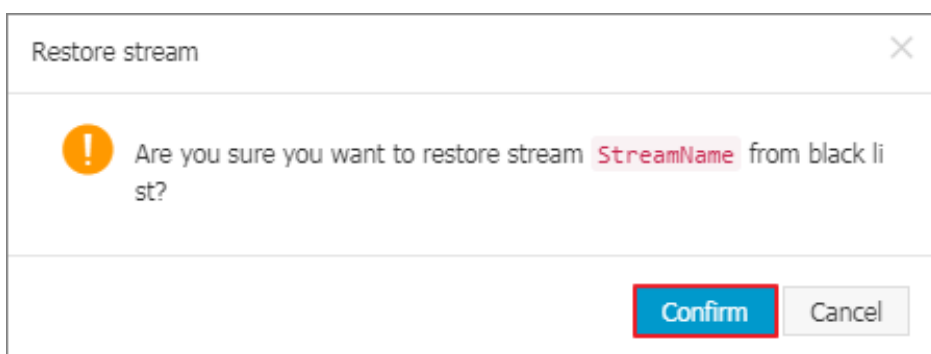
Select **BlackList**.

Select the address.

Click **Restore** from the **Actions** column, from the selected address.



Click **Confirm**.



The address is restored from the blacklist successfully.

Playback address

Live video addresses can be classified into original image addresses and transcoded addresses.

Original image address

Original images are original video streams that are not transcoded. The original image address is in the format of Playback domain name+AppName+StreamName.

Alibaba Cloud provides three playback protocols that can be applied to the multiple terminals and platforms.

	Advantage	Disadvantage	Latency	Feature	Applicable terminal
RTMP	Low latency	Unstable during high concurrency Players that support related protocols must be developed for iOS. Usage of the non-standard TCP ports	1s to 3s	TCP persistent connection	PC end
HLS	Cross-platform Playing using HTML5	High latency	>10s	HTTP short connection	PC end and mobile end

	decompress ed packet				
HTTP-FLV	Low latency Playing using HTML5 decompress ed packet	Playing through the integrated SDKs	1s to 3s	TCP persistent connection	PC end

Playback addresses of different specifications:

RTMP format: `rtmp:// live.aliyun.com/{AppName}/{StreamName}`

FLV format: `http:// live.aliyun.com/{AppName}/{StreamName}.flv`

M3U8 format: `http:// live.aliyun.com/{AppName}/{StreamName}.m3u8`

Example

The streaming address is:

`rtmp://video-center.alivecdn.com/{live}/{3}?vhost={Live video domain name}`

The corresponding playback addresses are:

`http:// play.aliyunlive.com/{live}/{3}`

`http:// play.aliyunlive.com/{live}/{3}.flv`

`http:// play.aliyunlive.com/{live}/{3}.m3u8`

Transcoding template

The ApsaraVideo Live transcoding service provides **NarrowbandHD templates**.

The **NarrowbandHD template** relies on Alibaba Cloud' s proprietary narrowband HD image processing technology to achieve a higher compression ratio while maintaining the same image quality and saving more live broadcast traffic.

Playback address

Rule of playback address splicing:Live video domain name+AppName+StreamName+Transcoding template ID

Transcoded template IDs corresponding to different specifications and templates:

Template\Speci	LD	SD	HD	UHD
----------------	----	----	----	-----

Configuration				
Original image	None	None	None	None
High-quality transcoding template	ld	sd	hd	ud

Example of playback address splicing:

RTMP format: `rtmp://+{Live video domain name}+/{AppName}+/{StreamName}+{Transcoding template ID}`

Example: `rtmp://live.aliyunlive.com/AppName/StreamName_sd`

FLV format: `http://+{Live video domain name}+/{AppName}+/{StreamName}+{Transcoding template ID}.flv`

Example: `http://live.aliyunlive.com/AppName/StreamName_sd.flv`

M3U8 format: `http://+{Live video domain name}+/{AppName}+/{StreamName}.m3u8`

Example: `http://livetest01.aliyunlive.com/AppName/StreamName.m3u8`

Note: Currently playback in the M3U8 format is not supported.

Template parameters

Template name	Template ID	Resolution (self-adaptive height and width)	Bit rate (kbps)
LD	ld	360	≤420
SD	sd	432	≤580
HD	hd	648	≤1100
UHD	ud	1080	≤1900

Restrictions

Each domain name supports a maximum of two channels of transcoding concurrent streams. That is, a maximum of two channels of live broadcast using transcoding templates can be

conducted under one domain name.

If the provided ApsaraVideo Live service cannot meet your current business needs, you can open a ticket to describe your needs or contact your customer service manager.

Transcoding rules

ApsaraVideo Live supports latency-based transcoding. If the system detects that a channel of live stream is not being watched, the system does not perform transcoding. If the system detects watching behavior, transcoding is immediately performed. Transcoding stops if no watching behavior is detected in 10 minutes.

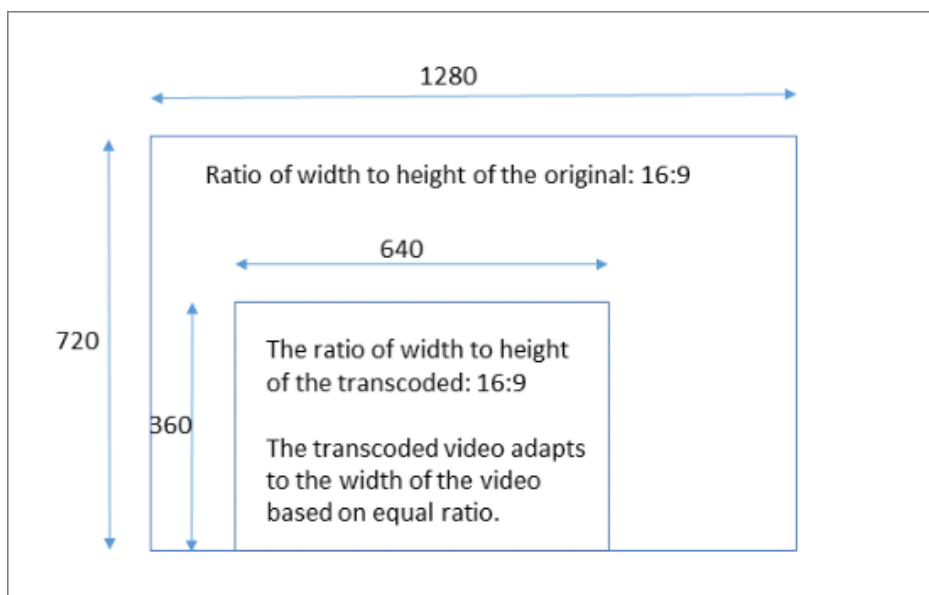
After a channel of video is transcoded, transcoded video is played for viewers.

Transcoding is a not required service. You can configure transcoding as needed.

- Currently transcoding supports FLV and RTMP formats.

Width self-adaptation

Transcoding uses self-adaptive width algorithms. Width of transcoded video is self-adaptive according to the height of the original streaming video.



Procedure

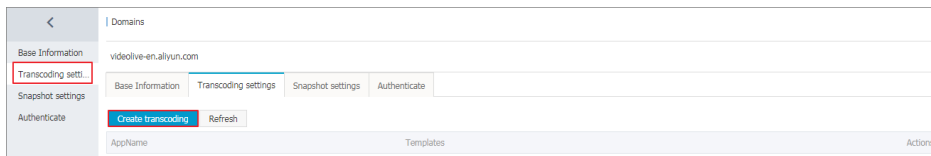
Log on to the ApsaraVideo Live console.

Select the region.

Select the domain name and click **Detail** from the **Actions** column.



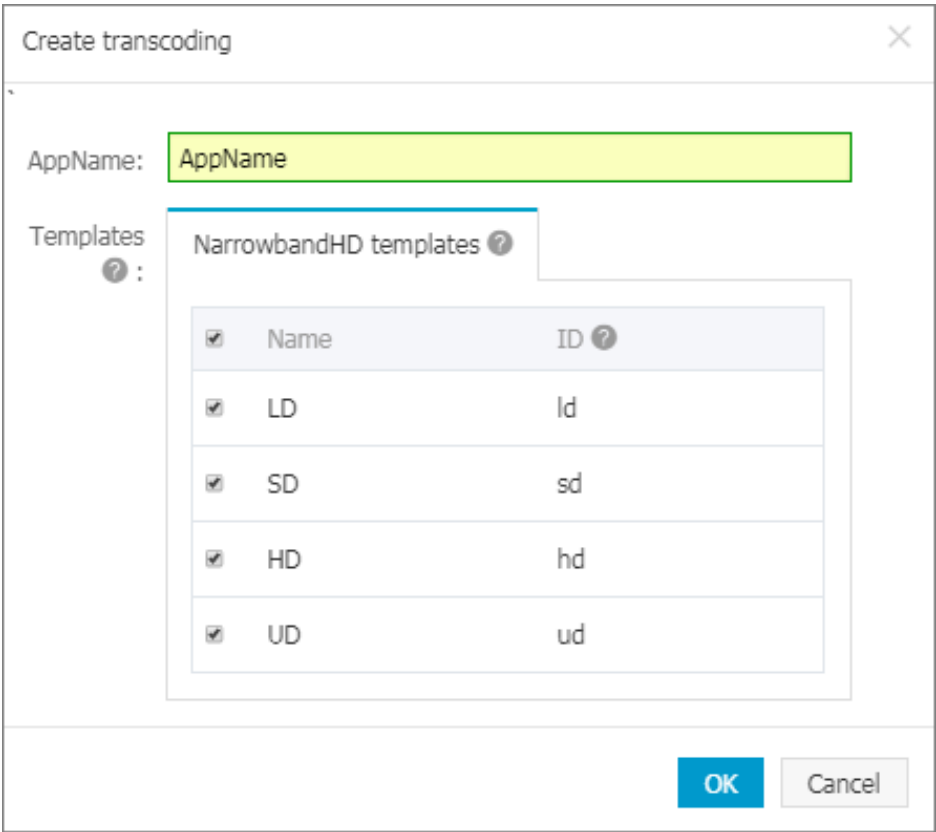
Click **Transcoding settings** and click **Create transcoding**.



Set the transcoding parameters and click **OK**.

Enter the AppName.

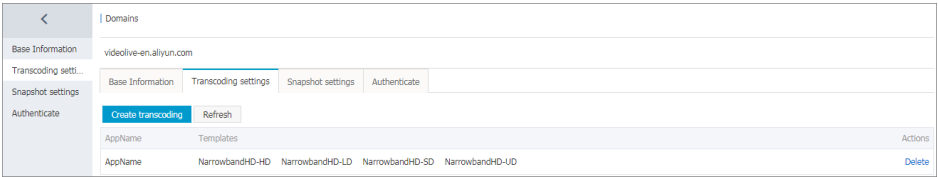
The transcoding template becomes effective only when the entered AppName matches that in the streaming address.



Select the transcoding template name.

Note: The high-quality (narrowband HD) transcoding template contains four transcoding templates: LD, SD, HD, and UHD.

The transcoding template is created.



Video playback.

After the transcoding template is created, you can perform video streaming. Video transcodes automatically according to the transcoding template. The transcoded video can be previewed on the ApsaraVideo Live console.

For more details about live video streaming, see [Live video streaming](#).

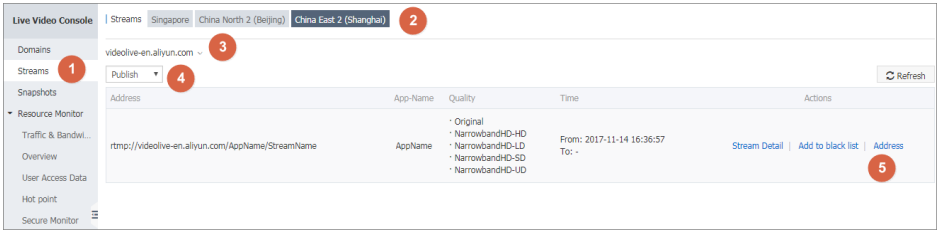
Click **Streams** in the left-side navigation pane.

Select the region.

Select the domain name.

Select the stream status from the drop-down list.

Select the streaming address, and click **Address** from the **Actions** column.



The playback addresses of the transcoded video and original video are displayed in the address list.

Hover the cursor over an address, the **Copy** and **Play** link are displayed.

Click **Copy** > **Confirm**. To play the video, paste the address in the address field. You can also click **Play** to play the video in the dialog box of the web player.

Address
✕

● Playing video will cause t

http://videolive-en.aliyun.c
 om/AppName/StreamName
 _ud.flv?auth_key=1510652
 806-0-0-3d820b48ab79fc8d
 f35b9ac1397b0ebc

NarrowbandHD-UD	RTMP Format: <i>rtmp://videolive-en.aliyun.com/AppName/StreamName_...</i> FLV Format: <i>http://videolive-en.aliyun.com/AppName/StreamName_...</i>	<div style="border: 1px solid red; padding: 2px 5px; display: inline-block;">Copy</div> <div style="border: 1px solid red; padding: 2px 5px; display: inline-block; margin-left: 5px;">Play</div>
NarrowbandHD-HD	RTMP Format: <i>rtmp://videolive-en.aliyun.com/AppName/StreamName_...</i> FLV Format: <i>http://videolive-en.aliyun.com/AppName/StreamName_...</i>	
NarrowbandHD-SD	RTMP Format: <i>rtmp://videolive-en.aliyun.com/AppName/StreamName_...</i> FLV Format: <i>http://videolive-en.aliyun.com/AppName/StreamName_...</i>	
NarrowbandHD-LD	RTMP Format: <i>rtmp://videolive-en.aliyun.com/AppName/StreamName_...</i> FLV Format: <i>http://videolive-en.aliyun.com/AppName/StreamName_...</i>	
Original	RTMP Format: <i>rtmp://videolive-en.aliyun.com/AppName/StreamName?...</i> FLV Format: <i>http://videolive-en.aliyun.com/AppName/StreamName....</i> M3U8 Format: <i>http://videolive-en.aliyun.com/AppName/StreamName....</i>	

OK

Snapshot management

Live video snapshot service supports taking snapshots of the live video being played at a set interval and saving the snapshots as .jpg files to a specified location in OSS.

Under a live video CDN domain, the live snapshot settings are differentiated by the AppName of the live video streaming. That is, streams under the same AppName all perform snapshot operations following the settings of this AppName. The AppName can be set to *, indicating that all the streams

under the live video CDN domain follow the snapshot settings.

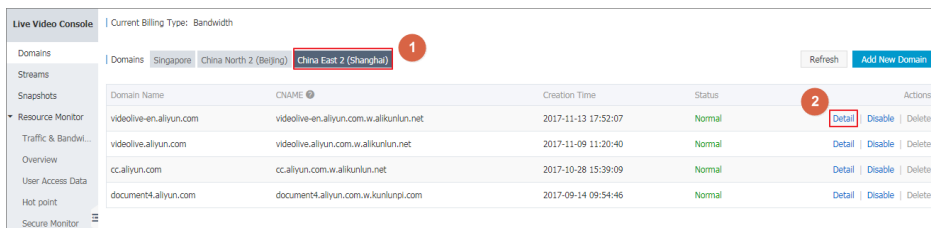
To conveniently view the snapshots, set a bucket for storage first.

Procedure

Log on to the ApsaraVideo Live console.

Select the region.

Select the domain name and click **Detail** from the **Actions** column.

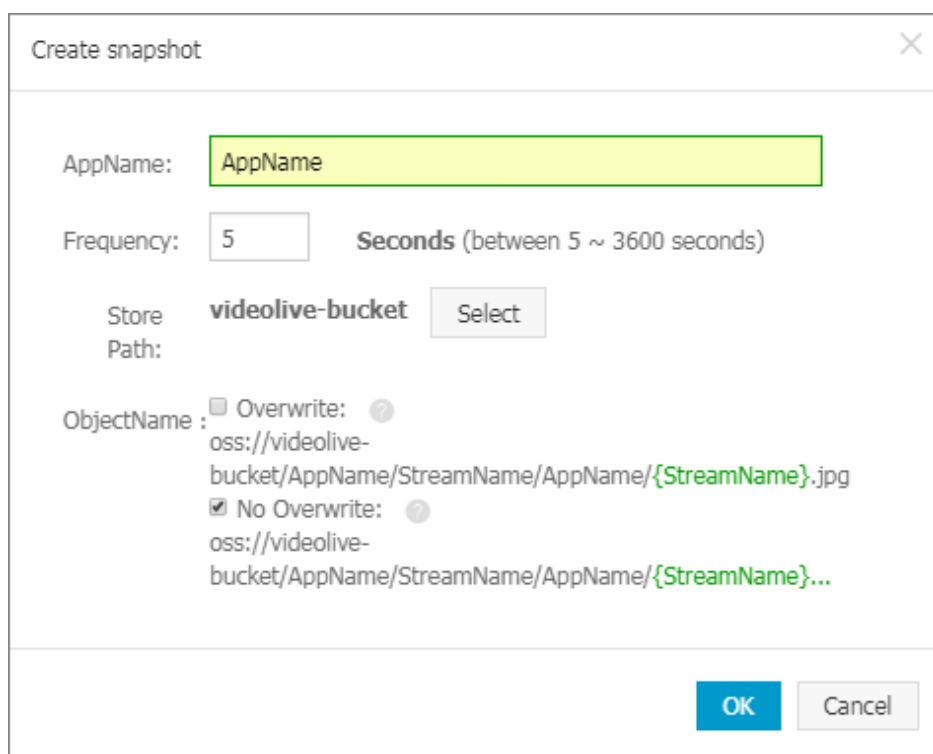


Click **Snapshot settings**.

Click **Create snapshot**.



Set the snapshot parameters and click **OK**.



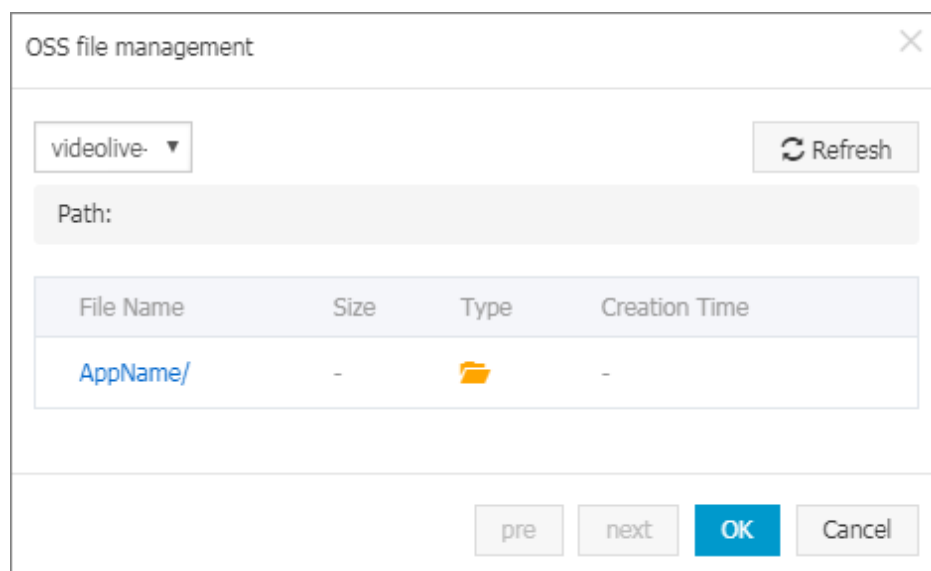
The 'Create snapshot' dialog box contains the following fields and controls:

- AppName:** A text input field with the placeholder text 'AppName'.
- Frequency:** A numeric input field with the value '5', followed by the text 'Seconds (between 5 ~ 3600 seconds)'.
- Store Path:** A dropdown menu showing 'videolive-bucket' and a 'Select' button.
- ObjectName:** A section with two options:
 - ☐ **Overwrite:**
oss://videolive-bucket/AppName/StreamName/AppName/{StreamName}.jpg
 - ☒ **No Overwrite:**
oss://videolive-bucket/AppName/StreamName/AppName/{StreamName}...
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Enter the **AppName** for which the snapshot function must be enabled.

Enter the frequency. It is the snapshot interval. It can be between 5 and 3,600 seconds.

Select the bucket in which the snapshot files are stored, and click **OK**.



The 'OSS file management' dialog box contains the following elements:

- Bucket Selection:** A dropdown menu showing 'videolive-' and a 'Refresh' button.
- Path:** A text input field.
- Table:** A table with columns 'File Name', 'Size', 'Type', and 'Creation Time'. It contains one row with the value 'AppName/' in the 'File Name' column, '-' in the 'Size' column, a folder icon in the 'Type' column, and '-' in the 'Creation Time' column.
- Buttons:** 'pre', 'next', 'OK', and 'Cancel' buttons at the bottom right.

Note: The bucket and the current domain name must be in the same region. For example, if the current domain name is located in **China East 2**

(Shanghai), the bucket must also be located in **China East 2 (Shanghai)**. If no bucket list is available in the panel, check that the OSS bucket and the domain name are in the same region.

Select a snapshot type, **Overwrite** or **No Overwrite**. Multiple types can be selected.

Overwrite: The video snapshots are taken in sequence based on the set interval, and the new snapshot can overwrite the older one.

No Overwrite: The video snapshots are taken in sequence based on the set interval, and the new snapshots are stored in OSS in the order of N+1 (N ≥ 0).

All snapshot settings under the domain name are listed on the **Snapshot settings** tab. For example, the snapshots of all the live video streams with AppName as the app name under the domain name are captured and exported according to this rule.

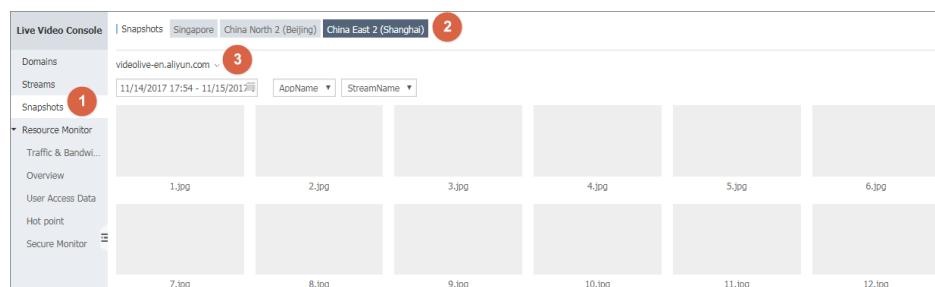
Note: The modified snapshot settings are applied to the next live video streaming.

Log on to the ApsaraVideo Live console.

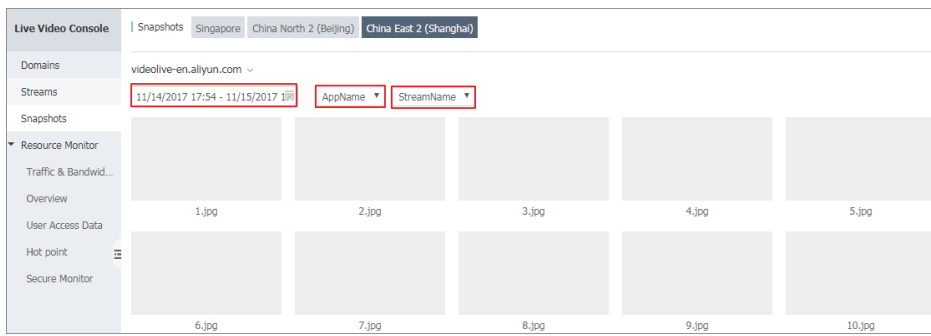
Click **Snapshots** in the left-side navigation pane.

Select the region.

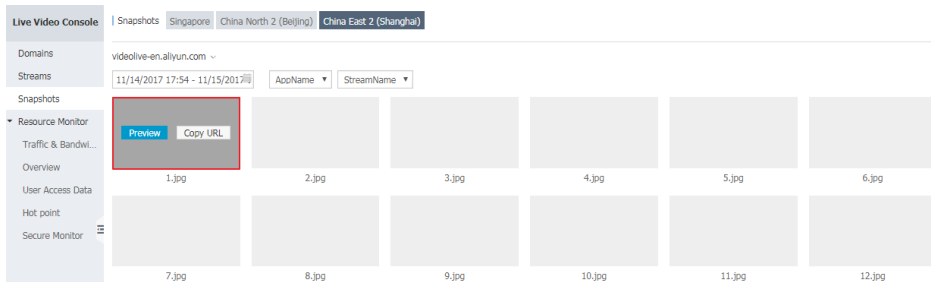
Select the domain name.



Enter the expected time period, and select the AppName and StreamName from the drop-down list. The snapshots list is displayed on the basis of your selection.



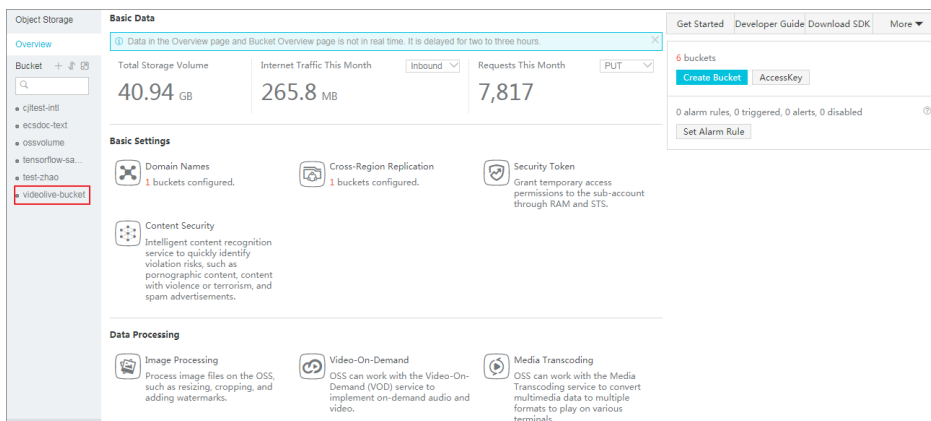
Hover your cursor over a snapshot in the list. Buttons to enlarge the image and copy the URL are displayed. You can perform the operations as required.



You cannot delete the snapshots directly in the ApsaraVideo Live console. Instead, you must perform the deletion operation in the OSS console.

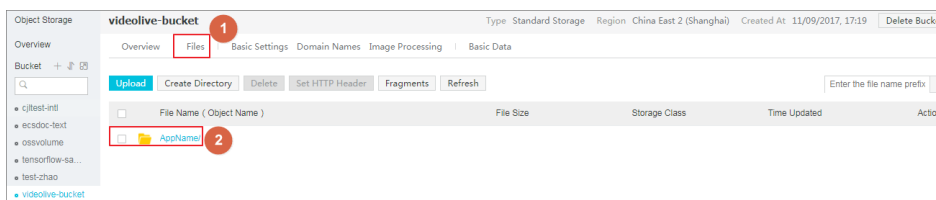
Log on to the OSS console.

On the **Overview** page, select the bucket where the snapshots are stored and click its name.



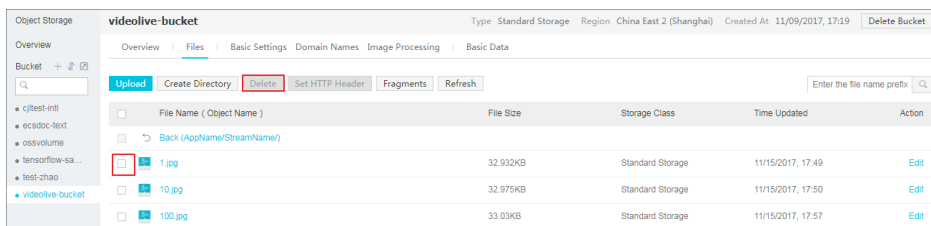
Click **Files**.

Select the folder name.

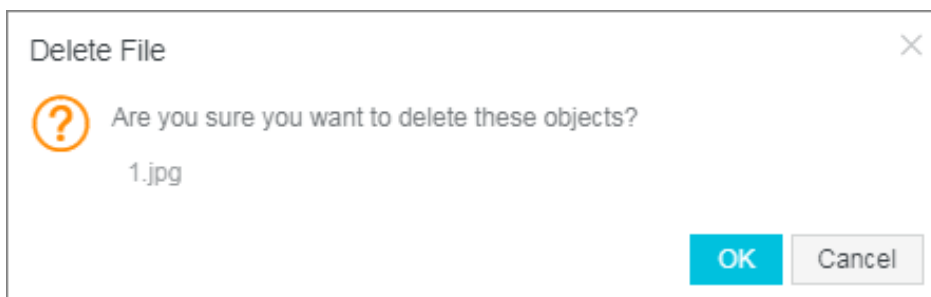


Select the snapshot to be deleted, and click **Delete**.

To delete multiple snapshots at once, select multiple snapshots and click **Delete**.



Click **OK**.



Note: To verify whether the selected snapshot has been deleted, you must return to the **snapshots** page of the ApsaraVideo Live console.

What is RAM

Through Alibaba Cloud Resource Access Management (RAM), you can provide required permissions to the subaccounts for the live broadcast in the ApsaraVideo Live console.

One primary account can create multiple subaccounts. By authorizing the subaccounts certain access functions, you can restrict their use of resources and functions for the purpose of unified management. For more information, see **What is RAM**.

Subaccount permissions mainly include authorization to use ApsaraVideo Live and OSS and CDN resource objects. We recommend that you plan the resource instances of such services for a subaccount, create authorization policies based on the corresponding authorization templates, and then grant the permissions to the subaccount.

RAM restrictions

RAM users cannot possess resources and they are not billed independently. These users are centrally controlled and billed under your Alibaba Cloud account. You can create separate passwords or keys for each RAM user, but these users do not have any operation permissions by default. RAM provides an access-policy-based authorization to help you grant fine-grained authority to the RAM users.

You must grant the following permissions to your subaccounts to use ApsaraVideo Live console functions:

Live (Required): Grants permission to use ApsaraVideo Live and uses the built-in **AliyunLiveFullAccess** authorization policy;

OSS (Required): Grants permission to use the screenshot storage service, which can be customized as needed;

CDN (Required): Grants permission to play videos, which can be customized as needed.

Authorization operations

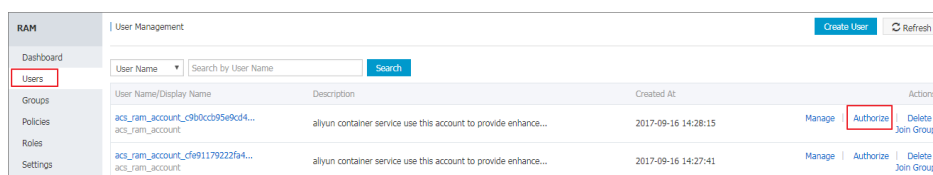
Authorization on ApsaraVideo Live

If a subaccount is required to use ApsaraVideo Live, you must grant the subaccount the permission to use ApsaraVideo Live. You can directly use the built-in **AliyunLiveFullAccess** authorization policy as follows:

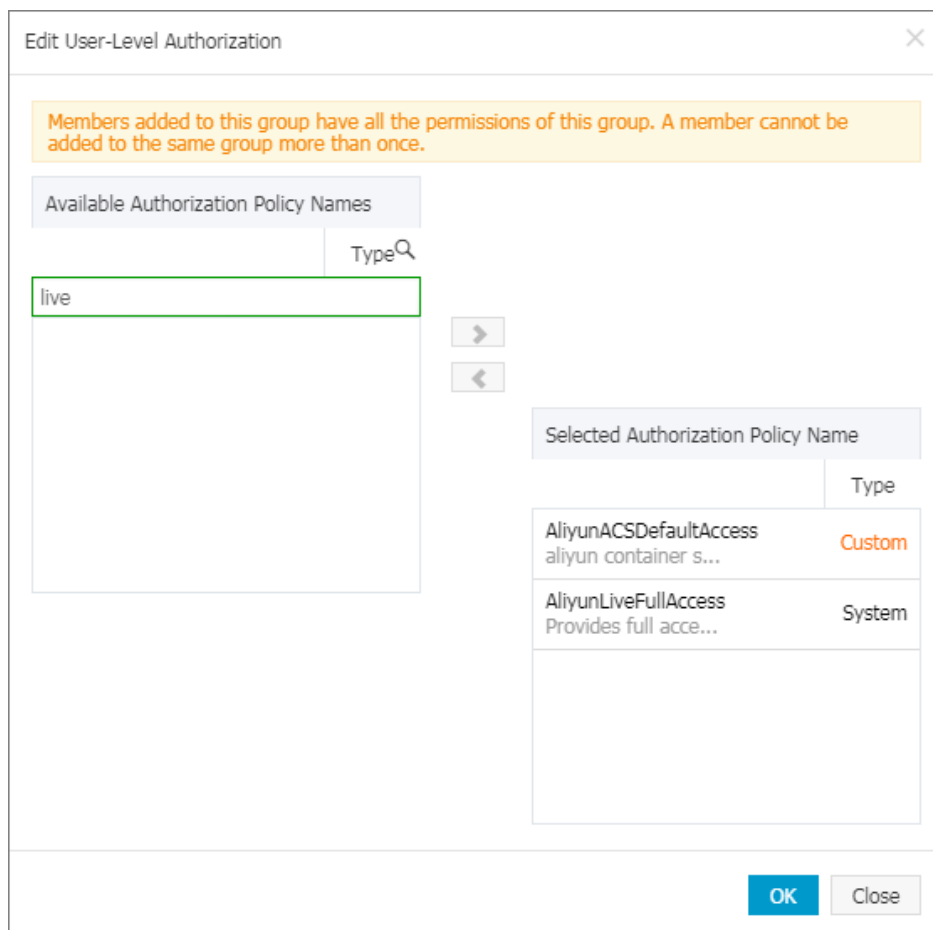
Log on to the RAM console.

Click **Users**.

Select **User Name** and click **Authorize** from the **Actions** column to grant the **AliyunLiveFullAccess** permission to the specified subaccount.



User Name (Display Name)	Description	Created At	Actions
acs_ram_account_c9b0ccb95e9cd4...	aliyun container service use this account to provide enhance...	2017-09-16 14:28:15	Manage Authorize Delete Join Group
acs_ram_account_cf691179222fa4...	aliyun container service use this account to provide enhance...	2017-09-16 14:27:41	Manage Authorize Delete Join Group



Description of custom authorization policy creation

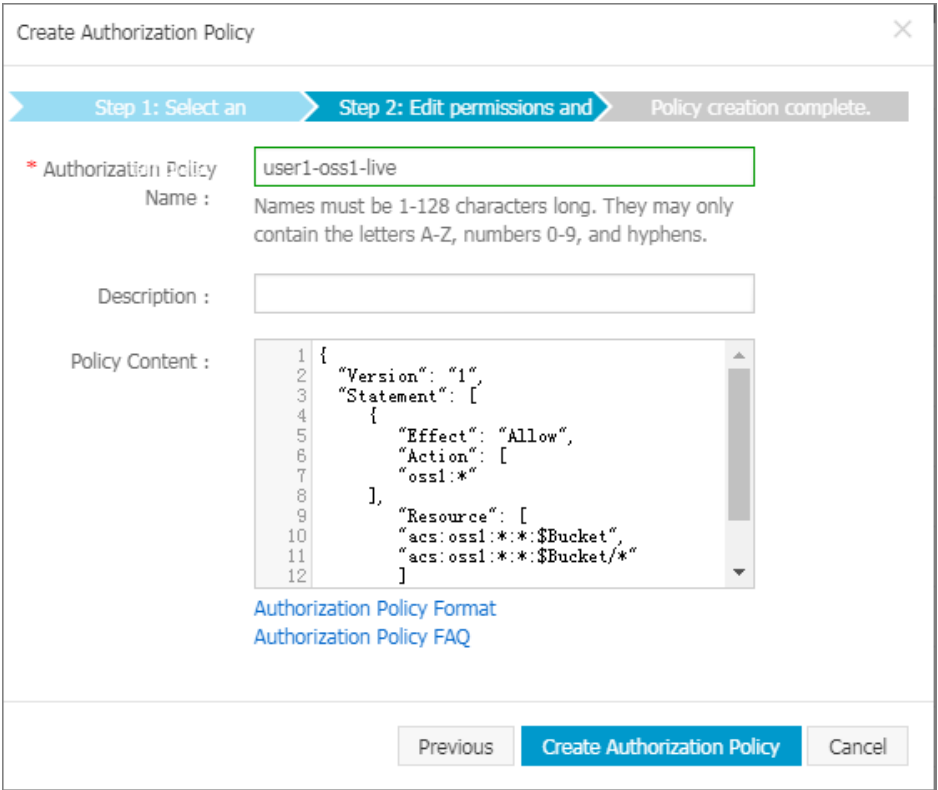
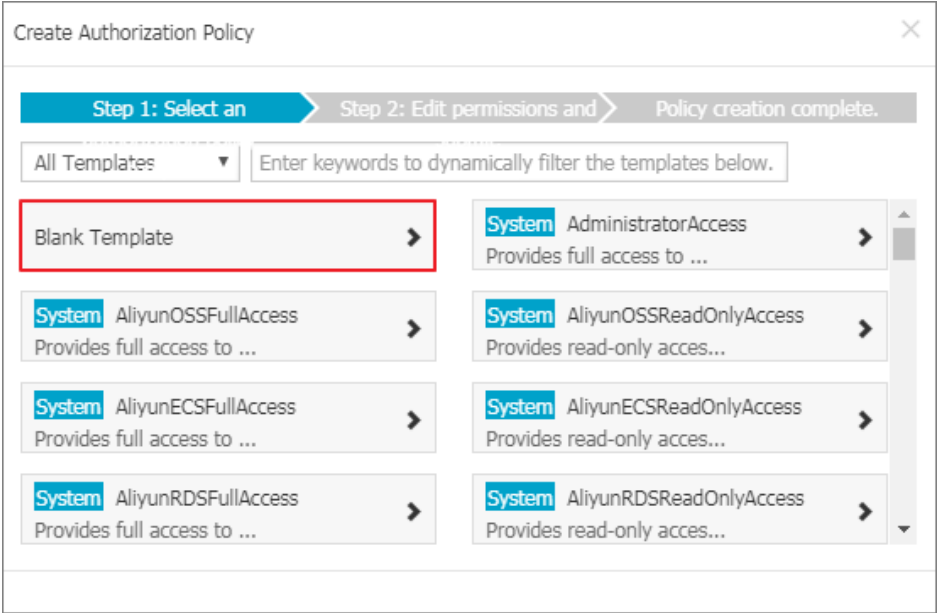
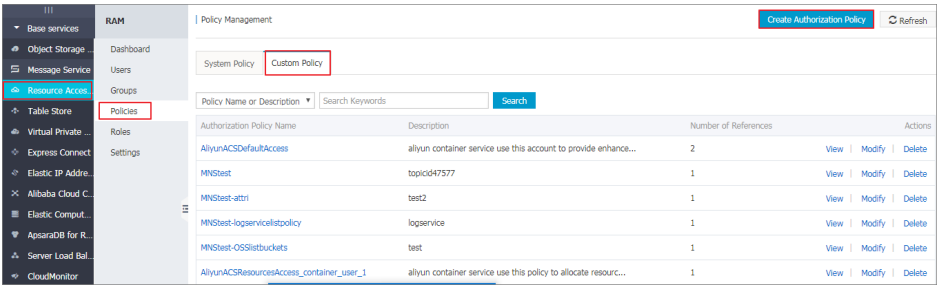
You can customize authorization policies and assign them to specified subaccounts as follows:

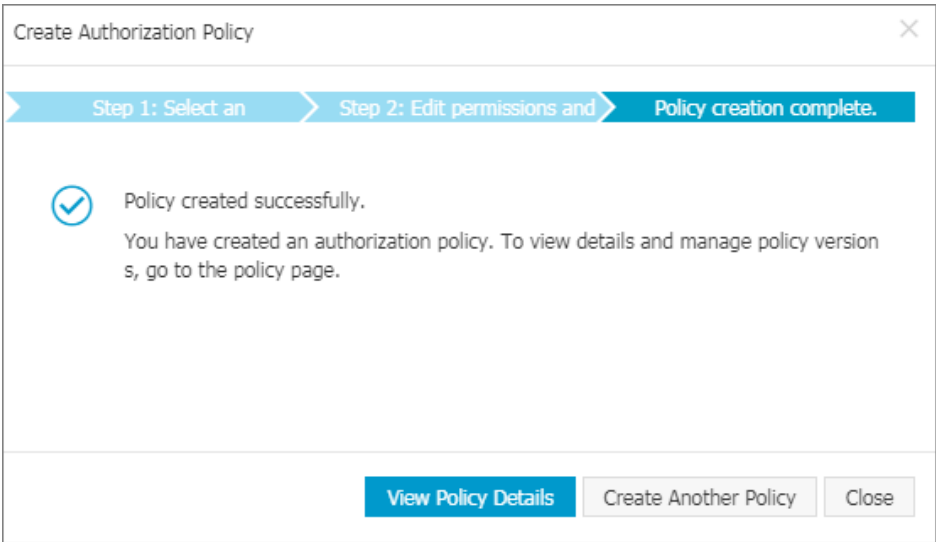
Log on to the RAM console.

Click **Policies**.

Click **Custom Policy**.

Click **Create Authorization Policy** to create custom authorization policies as the following samples for the specified resource instance and grant the policies to the specified subaccount.





Policy Management				Create Authorization Policy	Refresh
System Policy Custom Policy					
Policy Name or Description		Search Keywords	Search		
Authorization Policy Name	Description	Number of References	Actions		
AliyunACSDefaultAccess	aliyun container service use this account to provide enhance...	2	View	Modify	Delete
MNStest	topicid47577	1	View	Modify	Delete
MNStest-attri	test2	1	View	Modify	Delete
MNStest-logservicepolicy	logservice	1	View	Modify	Delete
MNStest-OSSlistbuckets	test	1	View	Modify	Delete
AliyunACSResourcesAccess_container_user_1	aliyun container service use this policy to allocate resourc...	1	View	Modify	Delete
user1-oss1-live		0	View	Modify	Delete

Note: After the authorization policies are created for various service resource objects, you can grant the permissions to the corresponding subaccounts.

The following are OSS and CDN authorization policies. You can grant corresponding permissions to subaccounts as needed.

OSS authorization policy

Permission description:

All operation permissions on specified buckets;
Permission to view the bucket list;

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "oss:*"
      ],
      "Resource": [
```

```

"acs:oss:*:*:$Bucket",
"acs:oss:*:*:$Bucket/*"
],
"Effect": "Allow"
},
{
  "Action": [
    "oss:ListBuckets"
  ],
  "Resource": "*",
  "Effect": "Allow"
}
]
}

```

CDN authorization policy

Permission description:

All permissions on specified CDN domains;
Permission to query CDN domains;

```

{
  "Version": "1",
  "Statement": [
    {
      "Action": "cdn:*",
      "Resource": [
        "acs:cdn:*:$Uid:domain/$DomainName"
      ],
      "Effect": "Allow"
    },
    {
      "Action": "cdn:Describe*",
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}

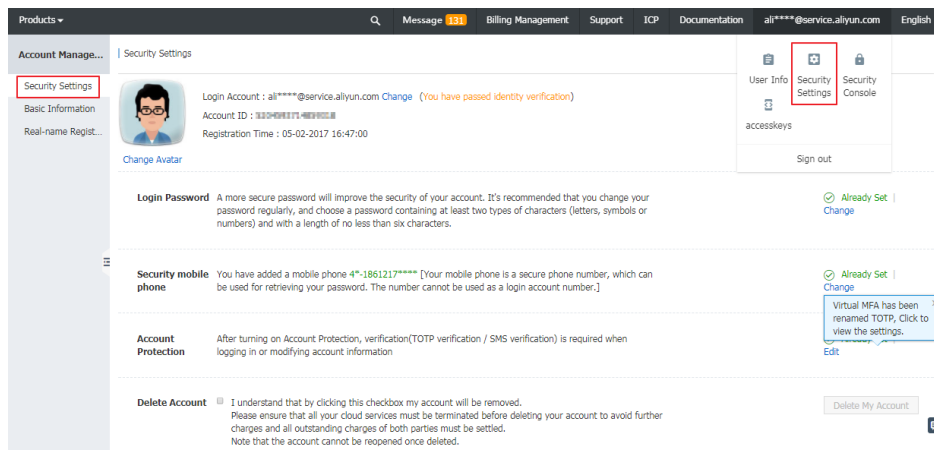
```

The following variables are used in the resource authorization policies of each service. Replace them with your actual resource instance name:

Description of variables

Uid

\$Uid: Alibaba Cloud account ID. You can query it through **Alibaba Cloud console > Account Management > Security Settings**.



Bucket

\$Bucket: OSS Bucket.

CDN

\$DomainName: Name of the CDN domain.

Resource monitoring

You can view the **traffic bandwidth**, **access overview**, **user access data**, **hot point**, and **security monitor** information on the ApsaraVideo Live console, and select the domain name and time segment to be monitored for each metric. Available metrics that you can monitor are as follows.

Monitoring Metric	Monitoring index
Traffic bandwidth	<ul style="list-style-type: none"> - Network bandwidth: The total traffic and peak bandwidth under the current domain name in the selected acceleration region and ISP within a certain time segment. - Origin retrieval bandwidth: The origin retrieval traffic monitored under the current domain name within a certain time segment. - Daily traffic statistics: Indexes for which statistics is performed daily, including the traffic, peak bandwidth, peak time point, peak origin retrieval bandwidth, peak origin retrieval bandwidth time point, and number of visits.
Access overview	<ul style="list-style-type: none"> - Hit rate: Traffic hit rate and request hit rate, among which, Traffic hit rate = Number of traffic that is hit/Total traffic; while Request hit

	<p>rate = Number of requests that are hit/Total requests.</p> <ul style="list-style-type: none"> - Access QPS: The number of accesses per second under the current domain name within a certain time segment. - HTTP CODE: The HTTP status code.
User access data	<ul style="list-style-type: none"> - PV: The number of times resource files under the current domain name are accessed within a certain time segment. - UV: The number of unique IP addresses that request resources under the current domain name within a certain time segment. - User region distribution: Distribution of users in terms of accessed sites, response time, and download speed under the current domain name within a certain time segment. - Carrier proportions: Shares of the carrier under the current domain name within a certain time segment.
Hot point	<ul style="list-style-type: none"> - Popular URLs: Popular URLs with a high number of access requests, and popular URLs with heavy traffic. - Popular referers: Popular referers with a high number of access requests, and popular referers with heavy traffic. - File response proportions: Response of files with a high number of access requests, and response of files with heavy traffic.
Security monitor	<ul style="list-style-type: none"> - CC monitoring: Number of attacks under the current domain name within a certain time segment.

You can select **Traffic&Bandwidth**, **Overview**, **User Access Data**, **Hot point** and **Security Monitor** from the **Resource Monitoring** page.

Log on to the ApsaraVideo Live consoleApsaraVideo Live console.

Click **Resource Monitor** in the left-side navigation pane.

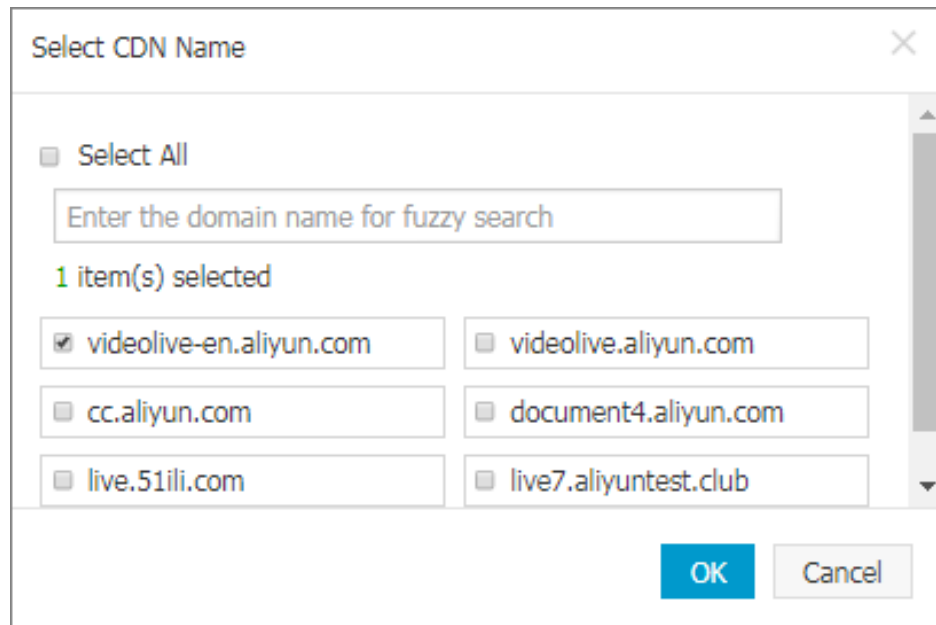
Click **Traffic&Bandwidth**.

Select **Monitored Domain Names**.

Click **Select CDN Name**.

Select the domain names.

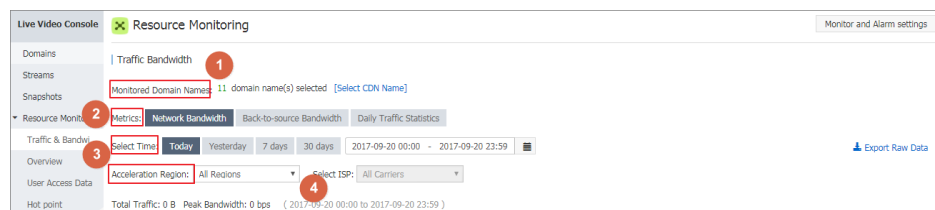
Click **OK**.



Select a monitoring metric.

Select the time period you want to monitor.

Select the acceleration region and ISP.



You can access **Monitor and Alarm settings** from **Traffic Bandwidth**, **Access Overview**, **Visitor Data**, **Hot Spot Analysis** or **Security Monitoring** pages.

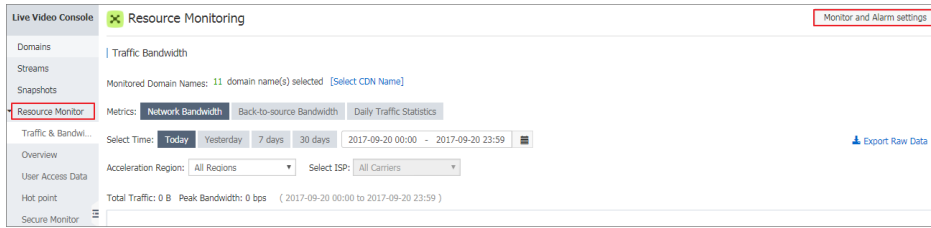
Procedure

Log on to the ApsaraVideo Live console.

Click **Resource Monitoring** in the left-side navigation pane.

Click **Traffic & Bandwidth**.

Click **Monitor and Alarm settings** in the upper-right corner to go to the CloudMonitor console.



Click **Alarm Rules**.

Click **Create Alarm Rule** in the upper-right corner to go to **Create Alarm Rule** page.

For more details, see [Alarm template best practices](#).

