ALIBABA CLOUD

阿里云

视图计算
知识库

文档版本：20210601

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.国标协议介绍

本文为您介绍《安全防范视图计算联网系统信息传输、交换、控制技术要求》的主要内容。

概述

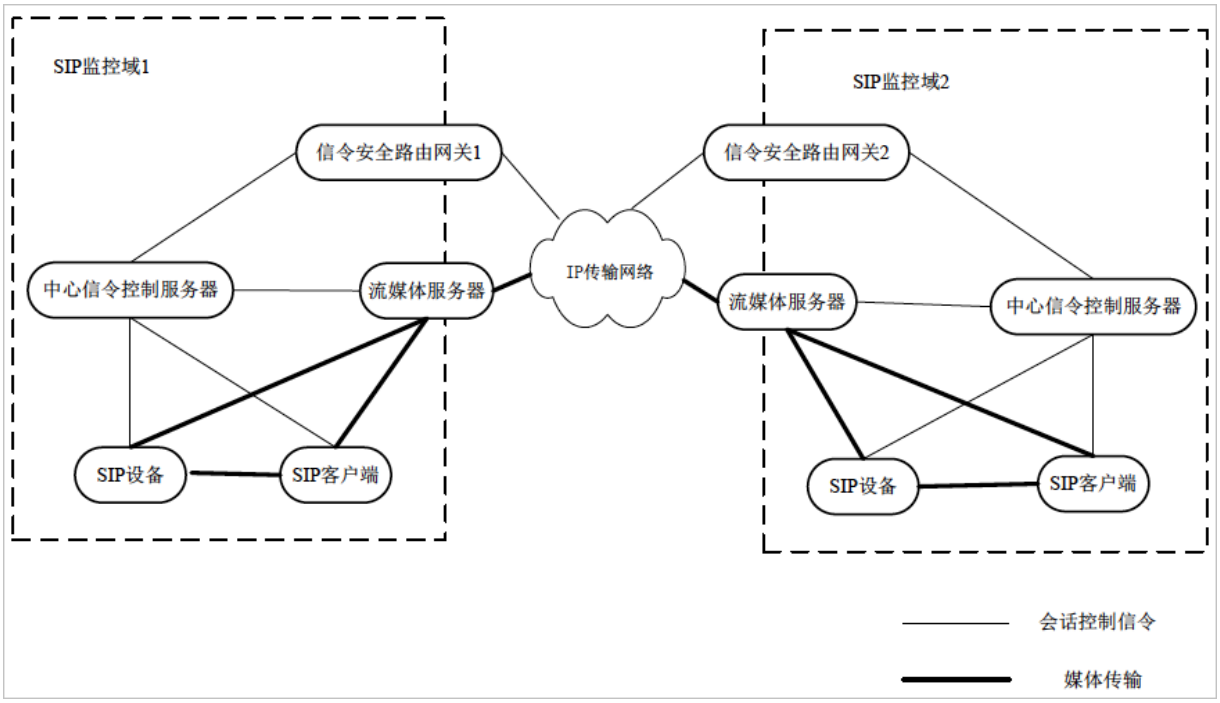
GB/T28181《安全防范视图计算联网系统信息传输、交换、控制技术要求》是由公安部科技信息化局提出，由全国安全防范报警系统标准化技术委员会（SAC/TC100）归口，公安部一所等多家单位共同起草的一部国家标准。 该标准规定了城市监控报警联网系统中信息传输、交换、控制的互联结构、通信协议结构，传输、交换、控制的基本要求和安全性要求，以及控制、传输流程和协议接口等技术要求。该标准适用于安全防范监控报警联网系统的方案设计、系统检测、验收以及与之相关的设备研发、生产，其他信息系统可参考采用。

自2011年推出GB/T28181-2011版本以来，全国安防行业都在建设部署基于GB/T28181标准的前端设备、平台服务器、平台客户端等安防产品。2016年又升级到GB/T28181-2016标准，该标准已成为国内安防行业主流协议规范。

以下对GB/T28181-2016做简要介绍。

SIP域互联

GB/T28181使用SIP协议进行信息传输、交互和控制，并定义了SIP监控域间互联、SIP监控域与非SIP监控域互联的结构。下图描述了在单个SIP监控域内、不同SIP监控域间两种情况下，功能实体之间的连接关系。功能实体之间的通道互联协议分为会话通道协议、媒体（本标准主要指视/音频）流通道协议两种类型。



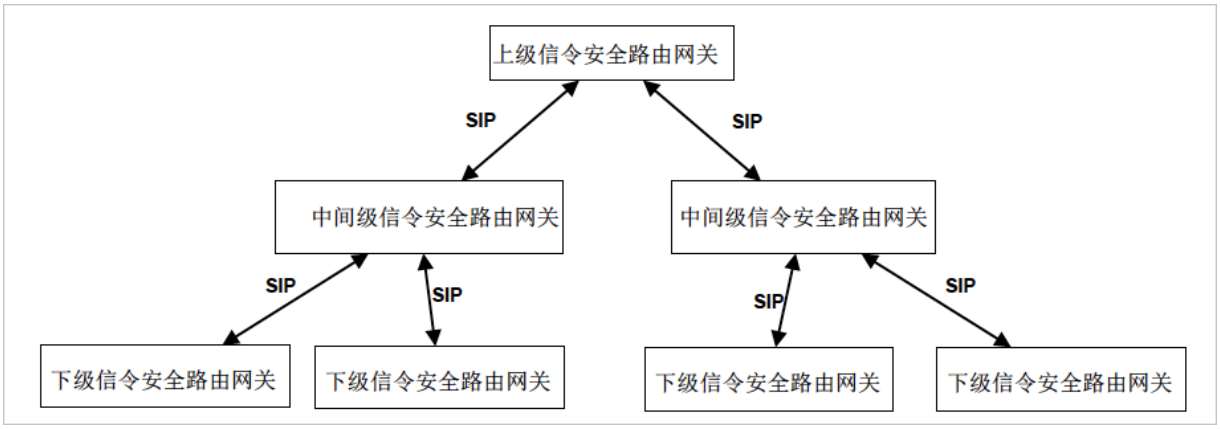
级联组网

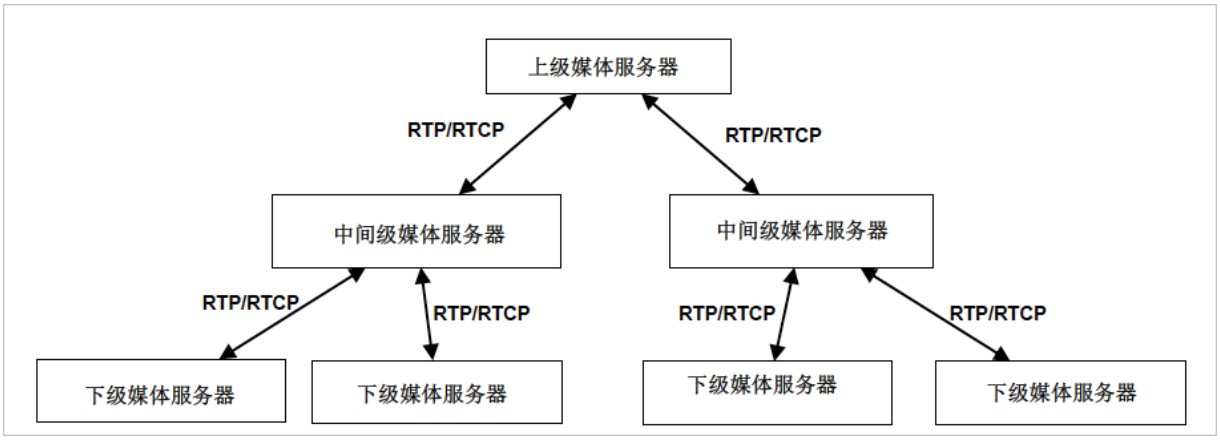
不同信令安全路由网关之间的组网方式分为级联和互联。

- 级联：两个信令安全路由网关之间是上下级关系，下级信令安全路由网关主动向上级信令安全路由网关。
- 发起注册，经上级信令安全路由网关鉴权认证后才能进行系统间通信。
- 互联：信令安全路由网关之间是平级关系，需要共享对方SIP监控域的监控资源时，由信令安全路由网关。

- 向目的信令安全路由网关发起，经目的信令安全路由网关鉴权认证后方可进行系统间通信。

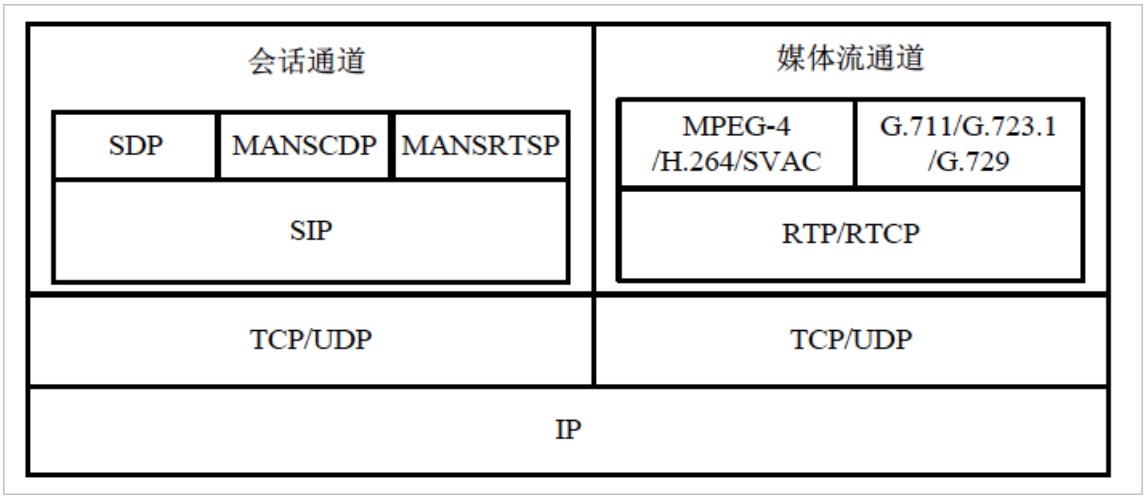
级联是较为常用的组网方式，下图描述了信令级联结构：





通信协议

联网系统内部进行视频、音频、数据等信息传输、交换、控制时，使用的通信协议结果如下：



联网系统在进行视音频传输及控制时应建立两个传输通道：会话通道和媒体流通道。会话通道用 于在设备之间建立会话并传输系统控制命令；媒体流通道用于传输视音频数据，经过压缩编码的视音 频流采用流媒体协议RTP/RTCP 传输。

控制协议

GB/T28181定义了一系列信息传输、交互、控制所需的协议，具体如下：

- 注册：应支持设备或系统进入联网系统时向SIP服务器进行注册登记的工作模式。
- 实时视音频点播：应支持按照指定设备、指定通道进行图像的实时点播，支持多用户对同一图像资源的同时点播。
- 设备控制：应支持向指定设备发送控制信息，如球机/云台控制、录像控制、报警设备的布防/撤防等，实现对设备的各种动作进行遥控。
- 报警事件通知和分发：应能实时接收报警源发送来的报警信息，根据报警处置预案将报警信息及时分发给相应的用户终端或系统、设备。
- 设备信息查询：应支持分级查询并获取联网系统中注册设备或系统的目录信息、状态信息等。
- 状态信息报送：应支持以主动报送的方式搜集、检测网络内的监控设备、报警设备、相关服务器以及连接的联网系统的运行情况。
- 历史视音频文件检索：应支持对指定设备上指定时间段的历史视音频文件进行检索。
- 历史视频频回放：应支持对指定设备或系统上指定时间的历史视音频数据进行远程回放，回放过程应支持正常播放、快速播放、慢速播放、画面暂停、随机拖放等媒体回放控制。
- 历史视音频文件下载：应支持对指定设备指定时间段的历史视音频文件进行下载。
- 网络校时：联网系统内的IP网络服务器设备宜支持NTP协议的网络统一校时服务。
- 订阅和通知：宜支持订阅和通知机制，支持事件以及目录订阅和通知。
- 语音广播和语音对讲：宜支持语音广播、语音对讲机制。
- 以上的控制协议在GB/T28181-2016中都有详细的控制过程定义。

参考资料

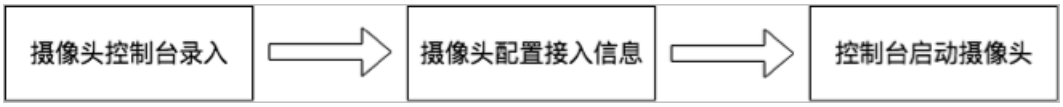
GB/T28181-2016《公共安全视图计算联网系统信息传输、交换、控制技术要求》。

2.国标协议接入流程

您可以通过本文了解国标协议接入流程。

国标注册流程说明

国标注册流程说明 国标设备（这里以摄像头为例）通过国标GB/T28181接入阿里云，需要现在 **视图计算** 的控制台录入摄像头信息，大致过程如下：



在摄像头自己的管理控制台页面，配置阿里云国标接入点配置信息。请注意查看NVR或IPC的配置（配置页面示意图如下），具体各型号的NVR或IPC配置说明请参照厂商提供的说明书。

1. 在GB/T28181的配置页面，“启用”框须勾选上。
2. 配置“SIP服务器ID”为阿里云视图计算产品提供的国标ID。
3. 配置“SIP服务器地址”和“SIP服务器端口”为阿里云视图计算产品提供的SIP服务器地址和端口（以上两步用到的阿里云视图计算产品国标信息在通过控制台或API在创建空间后可获取到）。
4. 协议版本设置为“GB/T28181-2016”。
5. 配置为基于TCP协议采用PS封装的视音频媒体传输。

国标接入配置示范

以下以某摄像头为例，详细示范操作步骤。

1. 在 视图计算控制台 的 空间管理页面，创建空间后，获取 空间信息 如下图右上方。
2. 点击导航栏的 空间监控，选择您要配置的空间， 单击 设备监控，点击 添加设备按钮。
3. 在添加设备详情页 如下图右下方相应处 填入对应项信息。

说明 支持设备通过TCP和UDP两种协议注册，可在摄像头国标注册页面选择TCP或UDP传输协议。同时考虑到网络传输链路上可能存在防火墙对5060等端口进行限制。阿里云视图计算接入网关支持UDP和TCP双协议多端口注册，UDP协议支持端口号5060、5160，TCP协议支持端口号6060、6160。

海康设备国标注册示范：

大华设备国标注册示范：

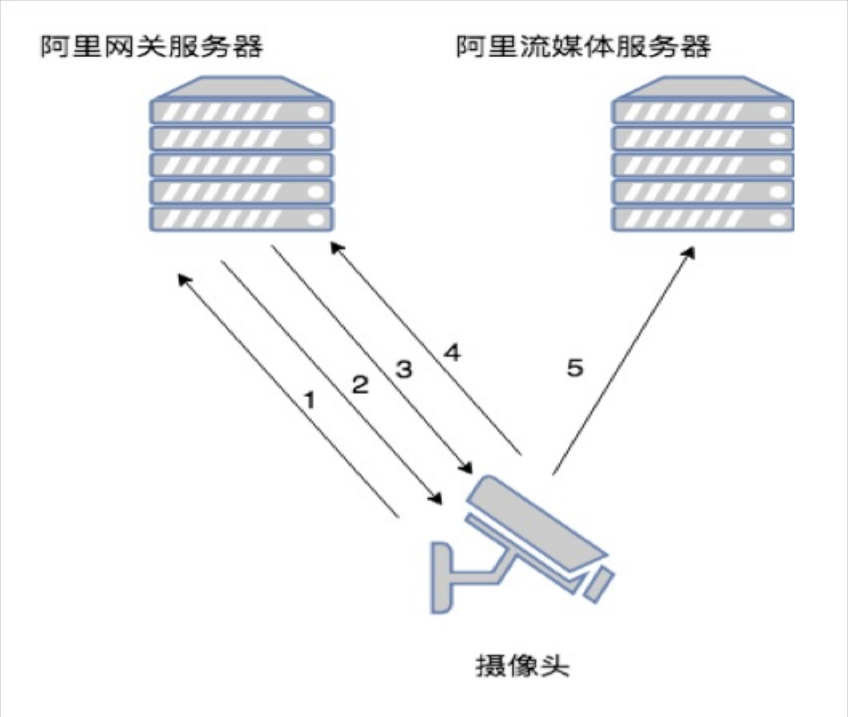
宇视设备国标注册示范：

说明

1. 请先在视图计算控制台添加设备，再在摄像头管理页面进行注册。
2. 在摄像头本身的管理页面，配置国标注册信息，其中必须填写的信息，请参考上图中标明数字对应的输入项。
3. 尤其需要注意国标注册的用户名和密码不是摄像头本身控制管理页面的登陆用户名和密码。国标注册的用户名需要和设备的国标ID保持一致。否则设备注册后会被锁定。需要分别在阿里云视图计算平台->设备监控->编辑页面更新设备用户名和密码，然后更新摄像头侧国标注册用户和密码信息，再点击“解锁”重新注册。

国标注册流程说明

在做好配置之后，摄像头将进行国标注册的流程，基本过程如下。



1. 摄像头发送注册请求到阿里SIP服务器。
2. 阿里SIP服务器认证通过之后回复200给摄像头，如果开启了认证，阿里SIP服务器会开始挑战模式，摄像头需要根据国标完成挑战之后重新注册才能通过认证。
3. 认证通过之后，开启摄像头拉流，阿里SIP服务器会发送INVITE国标请求到摄像头，其中携带了阿里流媒体服务器的地址信息。
4. 摄像头收到之后回复200。
5. 摄像头主动连接阿里流媒体服务器，并开始推送视频流。

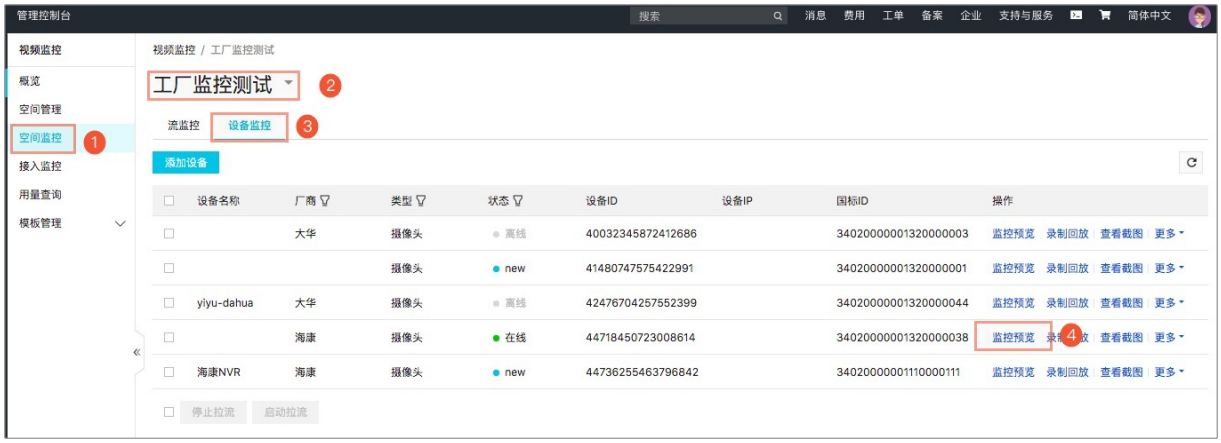
设备注册成功后启动拉流

1. 启动拉流

   国标注册成功后，如果设置了自动启动拉流则视图计算服务直接启动拉流，若未配置自动启动拉流，需要通过触发的方式来启动拉流（可通过控制台 **空间监控** -> **添加设备** 中设置 **添加后启动拉流** 或 **空间监控** -> **设备监控** 中选择启动拉流，或者API触发启动拉流。

2. 实时预览

   设备成功注册后，可以通过控制台的**空间监控** -> **设备监控**实时预览监控流。



控制台无法实时预览问题定位

- 确认摄像头平台设置中是使用GB/T28181-2016国标协议进行国标设备的注册。
- 由于控制台播放器不支持H.265视频播放，通过设置摄像头编码方式，改成H.264。如果修改国标摄像头接入编码方式从H.265改成H.264，以某摄像头为例修改视频编码方式步骤如下。

说明 如果使用RTMP推流方式，您的播放终端可以解码播放H.265视频，可以全程使用H.265编码进行接入、录制和播放，只不过在控制台不能实时预览和回看。国标目前不支持H.265编码监控流接入，计划将在12月支持。

3.RTMP协议接入流程

生成鉴权URLRTMP协议接入的流程与普通视频直播类似，需要首先准备好备案过的推流域名和播流域名。本文为您介绍具体操作流程。

RTMP推流

1. 准备好备案过的推流和播放域名。
2. 在**视图计算控制台**或**使用视图计算API**创建空间时填入推流和播流域名。
3. 空间创建成功后（保险起见，建议间隔30秒后），进行域名的CNAME配置。
4. 通过配置的推流域名按RTMP协议格式进行推流，假如我们的推流域名为 push.vs.aliyun.com，那么不带鉴权的推流地址为：rtmp://push.vs.aliyun.com/live/StreamName?（备注：视图计算产品默认使用live作为appname进行推流）。
5. 生成带鉴权的URL，出于安全考虑所有监控流都需要进行URL鉴权加密。
6. 支持RTMP协议的摄像头或智能设备使用上一步中的推流地址进行推流。
7. 对于正在进行的监控实时流，可以使用如下带鉴权的播放地址进行播放（播放地址鉴权URL生成原理与推流地址的鉴权URL生成原理相同），将任一地址填入支持直播流播放的工具软件拉流地址中，单击 开放播放 相关按钮进行播放。

RTMP实时监控流的播放

接入视图计算的实时流支持三种协议方式的播放：RTMP播放、HTTP FLV播放、HLS播放。

三种播放地址主要不同之处：

- 延迟：httpflv与rtmp延迟较小，适合低延时播放的场景，hls延迟较大但兼容性好，适合对延时不敏感但需要更多播放终端可以播放的场景。
- 兼容性：httpflv和rtmp需要flash播放器或则客户端播放器，hls可以直接在浏览器中播放。

RTMP、HLS、HTTP-FLV 协议对比

	优点	缺点	延时	特点	适合端
RTMP	延时低	高并发下不稳定 iOS 平台要开发支持相关协议的播放器 使用非标准 TCP 端口	1S～3S	TCP 长连接	PC 端
HLS	跨平台 可通过 html5 解封包播放	延时高	> 10S	HTTP 短连接	PC端、移动端
HTTP-FLV	延时低 可通过 html5 解封包播放	需要集成 SDK 才能播放	1S～3S	TCP 长连接	PC 端

4.视图计算安全篇之URL鉴权

本文为您介绍URL鉴权的工作原理。

为了保障监控视频流上云的安全性，防止接入域名/播放域名被非法盗取，内容被未经授权方播放，视图计算产品默认会对推流域名（RTMP推流使用），播流域名（RTMP、国标GB28181）进行URL鉴权。

通过防盗链方法添加 Referer 黑名单的方式可以解决一部分盗链问题。但是，由于 Referer 内容可以伪造，所以Referer 防盗链方式无法彻底保护站点资源。因此，采用URL鉴权方式保护用户监控资源更为安全有效。

工作原理

URL鉴权功能通过阿里云接入节点（监控设备的接入）和CDN加速节点与客户业务服务（客户的业务服务用来进行实时监控流、历史监控流的组织管理等操作）配合，实现了一种更为安全可靠的监控资源防盗方法。

- 客户业务服务端提供加密 URL（接入流/播放流URL，包含权限验证信息）。
- 您使用加密后的 URL 向阿里云接入点（监控流接入）或CDN加速节点（监控流播放）发起请求。
- 接入点或CDN加速节点对加密 URL 中的权限信息进行验证以判断请求的合法性。正常响应合法请求，拒绝非法请求。

操作步骤

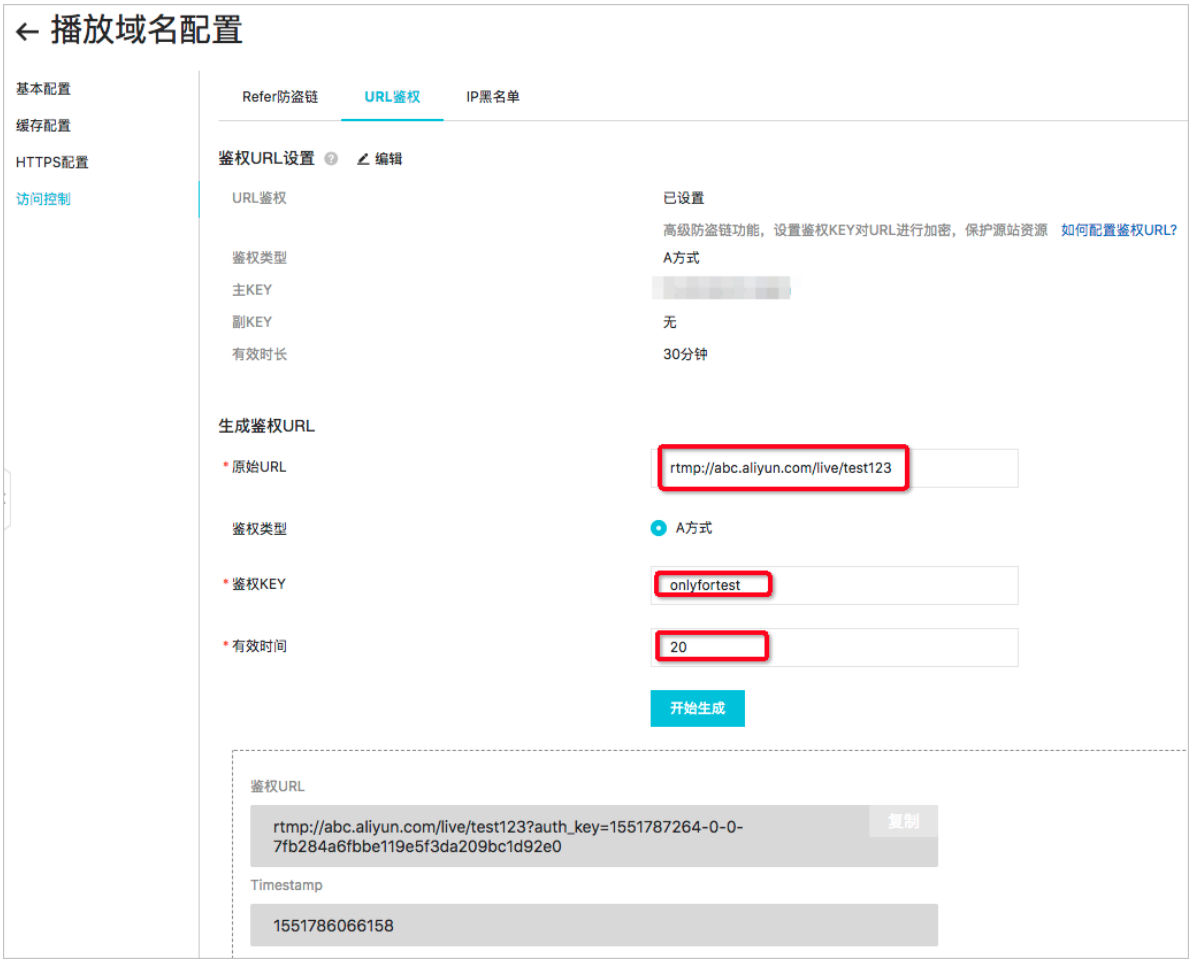
1. 在 **视图计算** 控制台页面下的 **空间管理** 页，选择一个空间，单击 **空间配置**。

2. 如果是RTMP协议接入，在推流域名和播放域名后面，单击 **域名配置** 分别配置URL鉴权，如果是国标GB28181协议接入，仅需配置播放域名的URL鉴权。

3. 在 **域名配置** 信息中，选择 **访问控制 **> URL鉴权**，填写 **鉴权KEY** 和 **鉴权时间** 来进行鉴权URL的设置。

- 生成鉴权URL Demo：填写原始URL、鉴权KEY和有效时间，系统生成一个完整的鉴权URL。此操作仅仅是操作示范，供您了解URL的完整格式，此鉴权URL不能直接进行使用。

  以下以RTMP播流URL鉴权为例：



- 如果是其他播放协议HTTP FLV，HLS或者推流URL鉴权，请在原始URL中输入对应的信息：
  - RTMP推流：`rtmp://pushtest.aliyun.com/live/firststream`
  - HTTP FLV播放：`http://companytest.aliyunlive.com/live/firststream.flv`
  - HLS播放：`http://companytest.aliyunlive.com/live/firststream.m3u8`

鉴权代码示例

视图计算的URL鉴权规则与视频直播URL鉴权原理类似，您可以参考鉴权代码示例。

5.常见问题诊断

您在使用视图计算时，您可查阅以下常见问题场景及解决方案。

摄像头注册不成功

摄像头注册不成功请按照如下步骤排查：

1. 检查摄像头所处的网络，是否能够连通SIP服务器的IP跟端口。
2. 检查摄像头所处的网络是否有防火墙，是否允许UDP包的收发。
3. 检查摄像头是否启用了国标28181的支持。
4. 检查摄像头里面的配置（注意不是控制台里有关摄像头的配置），查看SIP服务器的国标ID跟SIP服务器的IP跟端口是否正确。
5. 检查是否配置了SIP域，如果配置了请确保SIP域为SIP服务器ID的前10位数字。
6. 检查摄像头的用户名密码是否与控制台输入的匹配。
7. 如果用户名密码配置错误，在连续多次尝试注册失败之后该摄像头会被锁定，需要等一个小时后才会解除锁定，之后才能重新开始注册。

摄像头推流不成功

摄像头在注册成功之后推流不成功，请按如下步骤排查：

1. 检查控制台里面摄像头是否处于启动状态，如果没有，请在控制台里面启动摄像头。
2. 检查摄像头所在网络是否能够访问阿里云视图计算接入结点的IP和端口，阿里云视图计算的国标收流端口（以上IP和端口信息在国标注册交互过程中可获取）。
3. 检查摄像头的工作模式是否为Active，即摄像头需要主动TCP连接到阿里云服务器的端口并推流。

控制台无法实时预览问题定位

- 由于控制台播放器不支持H.265视频播放，国标设备接入可通过设置摄像头编码方式，改成H.264。RTMP接入请确认推流编码方式。如果您的终端可以播放H.265视频，可以全程使用H.265进行编码，只不过在控制台不能实时预览和回看。以某摄像头为例修改视频编码方式步骤如下。

- 如果是国标设备接入，确认摄像头平台设置中是使用GB/T28181-2016国标协议进行国标设备的注册。

摄像头视频流卡顿

摄像头在推流成功之后，视频流比较卡顿，请按如下步骤排查：

1. 检查摄像头里面的配置，查看当前摄像头推送的码流，因为摄像头是公网接入，请根据摄像头的实际网络情况选择合适码率的视频流。
2. 请检查播放所在的网络带宽是否满足摄像头的码率。

摄像头国标注册配置信息不正确

摄像头在国标注册前要在自己的管理页面上进行国标接入配置，需检查以下信息是否正确：

- 在GB/T28181的配置页面，“启用”框须勾选上。
- 检查“SIP服务器ID”是否为阿里云视图计算产品提供的国标ID。
- 检查“SIP服务器地址”和“SIP服务器端口”是否为阿里云视图计算产品提供的SIP服务器地址和端口。
- 检查协议版本是否为“GB/T28181-2016”。
- 配置为基于TCP协议采用PS封装的视音频媒体传输。

国标流接入失败排查步骤

- 检查与阿里云服务器的网络连接。可以采用telnet阿里云视图计算产品提供的SIP服务器地址和端口，或者直接在NVR或IPC侧抓包的方式检查。
- 检查国标注册是否成功。在NVR或IPC的国标配置页面上可能有注册成功与否的提示，具体信息请参考厂商手册。
- 检查国标信令交互。抓包查看是否会收到阿里云侧SIP服务器的INVITE请求，以及其中是否包含的阿里云侧媒体服务器地址和端口；NVR或IPC是否回复给阿里云侧SIP服务器INVITE请求。
- 检查视频接入是否成功。抓包查看NVR或IPC是否有数据发送给阿里云侧媒体服务器地址和端口，以及视频是否采用PS封装。

常见播放延时情况说明

- 目前已知VLC或者ffplay等播放器在播放rtmp或者flv的视频时，默认行为是分析5秒(rtmp)到90秒(以.flv做为后缀的url)数据查找媒体中是否包含音频。在无音频的流中，这一播放器行为会造成起播和播放的视频时间延迟。对于ffplay，可以加入参数"-analyzeduration 1"来实现秒开。另外，推荐使用aliplayer做为播放器实现秒开。

```
ffplay -analyzeduration 1 'http://edge1.example.com/app/ipc-1.flv?vhost=test.example.com'
```

- 除播放器造成的延时外，视频本身的GOP设置也会造成额外的延时。例如，GOP设为2秒，可能造成小于2秒的延时；如果播放时间点与上一关键桢相差1秒，则会造成1秒的延时。

直播播放常见问题参考

监控实时流问题诊断可适当参考视频直播中流播放相关问题诊断部分。

6.国标接入问题排查

本文档描述了国标设备接入常见问题的排查步骤。

摄像头注册不成功

摄像头注册不成功请按照如下步骤排查：

1. 检查摄像头所处的网络，是否能够连通SIP服务器的IP和端口。
2. 检查摄像头所处的网络是否有防火墙，是否允许UDP包的收发。
3. 检查摄像头是否启用了国标GB/T28181的支持。
4. 检查摄像头里面的配置（注意不是控制台里有关摄像头的配置），查看SIP服务器的国标ID、SIP服务器的IP和端口是否正确。
5. 检查是否配置了SIP域，如果配置了请确保SIP域为SIP服务器ID的前10位数字。
6. 检查摄像头的用户名密码是否与控制台输入的匹配。
7. 如果用户名密码配置错误，在连续多次尝试注册失败之后该摄像头会被锁定，需要等一个小时后才会解除锁定，之后才能重新开始注册。

摄像头推流不成功

摄像头在注册成功之后推流不成功，请按如下步骤排查：

1. 检查控制台里面摄像头是否处于启动状态，如果没有，请在控制台里面启动摄像头。
2. 检查摄像头所在网络是否能够访问阿里云结点的IP和端口（在国标信令交互时会返回此IP和端口）。
3. 检查摄像头的工作模式是否为Active模式。

摄像头视频流卡顿

摄像头在推流成功之后，视频流比较卡顿，请按如下步骤排查：

1. 检查摄像头里面的配置，查看当前摄像头推送的码流，因为摄像头是公网接入，请根据摄像头的实际网络情况选择合适码率的视频流。
2. 请检查播放所在的网络带宽是否满足摄像头的码率。

7.国标ID命名规范

本文为您介绍国标ID命名规范。

国标ID是在国标GB/T28181中使用的ID，在一个空间下保持唯一，命名规则应遵从GB/T 28181-2016《公共安全视图计算联网系统信息传输、交换、控制技术要求》。

国标ID由中心编码（8位）、行业编码（2位）、类型编码（3位）、网络标识（1位）和序号（6位）共20位十进制数字字符构成，其中：

- 中心编码指用户或设备所归属的监控中心编码，按照监控中心所在地的行政区划代码确定，当不是基层单位时空余为0，行政区划分代码采用GB/T 2260-2007规定的行政区划代码表示。
- 行业编码是指用户或设备所归属的行业，规则说明见“行业编码规则”。
- 类型编码指定了设备或用户的具体类型。
- 详细说明如下“详细规则说明”。

详细编码规则

码段	码位	含义	取值说明	
中心编码	1、2	省级编号	由监控中心所在地的行政区划代码确定，符合GB/T 2260-2007的要求。	
	3、4	市级编号		
	5、6	区级编号		
	7、8	基层接入单位编号		
行业编码	9、10	行业编码	行业编码	
类型编码	11、12、13	111～130 表示类型为前端主设备	111	DVR编码
			112	视频服务器编码
			113	编码器编码
			114	解码器编码
			115	视频切换矩阵编码
			116	音频切换矩阵编码
			117	报警控制器编码
			118	网络视频录像机（NVR）编码
			130	混合硬盘录像机（HVR）编码
			119～129	扩展的前端主设备类型

		131～199表示类型为前端外围设备	131	摄像机编码
			132	网络摄像机（IPC）编码
			133	显示器编码
			134	报警输入设备编码（如红外、烟感、门禁等报警设备）
			135	报警输出设备编码(如警灯、警铃等设备)
			136	语音输入设备编码
			137	语音输出设备
			138	移动传输设备编码
			139	其他外围设备编码
			140-199	扩展的前端外围设备类型
		200～299表示类型为平台设备	200	中心信令控制服务器编码
			201	Web应用服务器编码
			202	媒体分发服务器编码
			203	代理服务器编码
			204	安全服务器编码
			205	报警服务器编码
			206	数据库服务器编码
			207	GIS服务器编码
			208	管理服务器编码
			209	接入网关编码
			210	媒体存储服务器编码
			211	信令安全路由网关编码
			215	业务分组编码
			216	虚拟组织编码
			212～214,217～299	扩展的平台设备类型

		300～399表示类型为中心用户	300	中心用户
			301～343	行业角色用户
			344～399	扩展的中心用户类型
		400～499表示类型为终端用户	400	终端用户
			401～443	行业角色用户
			444～499	扩展的终端用户类型
		500～599表示类型为平台外接服务器	500	视频图像信息综合应用平台信令服务器
			501	视频图像信息运维管理平台信令服务器
			502～599	扩展的平台外接服务器类型
		600～999为扩展类型	600～999	扩展类型
网络标识	14	网络标识编码	0、1、2、3、4为监控报警专网，5为公安信息网，6为政务网，7为Internet网，8为社会资源接入网，9预留	
序号	15～20	设备、用户序号		

行业编码规范

接入类型码	名称	建设主体	备注
00	社会治安路面接入	政府机关	包括城市路面、商业街、公共区域、重点区域等
01	社会治安社区接入		包括社区、楼宇、网吧等
02	社会治安内部接入		包括公安办公楼、留置室等
03	社会治安其他接入		
04	交通路面接入		包括城市主要干道、国道、高速交通状况监视
05	交通卡口接入		包括交叉路口、“电子警察”、关口、收费站等
06	交通内部接入		包括交管办公楼等
07	交通其他接入		
08	城市管理接入		
09	卫生环保接入		
10	商检海关接入		
11	教育部门接入		
12～39			预留1
40	农林牧渔业接入	企业/事业单位	
41	采矿企业接入		
42	制造企业接入		
43	冶金企业接入		
44	电力企业接入		
45	燃气企业接入		
46	建筑企业接入		
47	物流企业接入		
48	邮政企业接入		
49	信息企业接入		
50	住宿和餐饮业接入		
51	金融企业接入		
52	房地产业接入		
53	商务服务业接入		
54	水利企业接入		
55	娱乐企业接入		
56～79			预留2
80～89		居民自建	预留3
90～99		其他主体	预留4

参考

- GB/T 28181-2016《公共安全视图计算联网系统信息传输、交换、控制技术要求》
- GB/T 2260-2007《中华人民共和国行政区划代码》

8.常用工具介绍

本文为您介绍视图计算的常用工具。

播放工具

常见的开源播放器有VLC、ffplay均支持主流的播放格式。另外rtmp或者flv格式的视频还可采用Adobe Flash Player播放。其中，ffplay可以通过加入命令行参数"-loglevel debug"的方式输出调试信息，便排查播放时出现的问题。

```
ffplay -loglevel debug -analyzeduration 1 'http://edge1.example.com/app/ipc-1.flv?vhost=test.example.com'
```

此外，还推荐使用aliplayer播放视图计算产品的视频，可以采用集成Web SDK的方式或者直接进行在线播放。详细信息请参阅：https://player.alicdn.com/ 。

常见网络分析工具

1. 1.采用telnet查看能否连接服务器端口：

   ```
   telnet <server> <port>
   ```

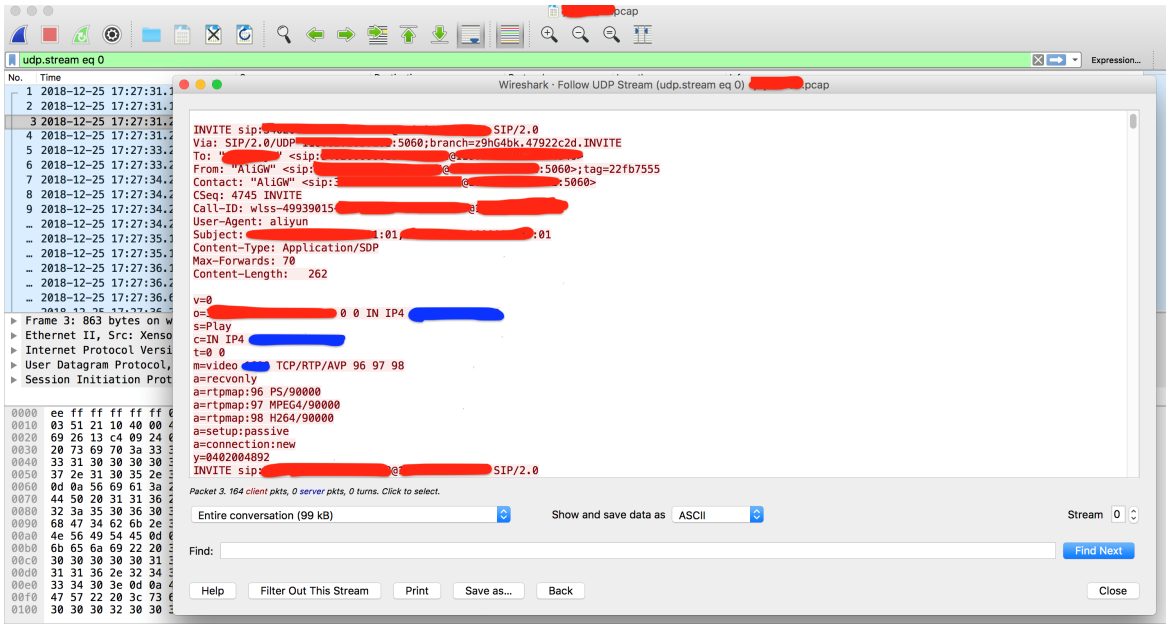
   例如：

   ```
   $ telnet 192.168.56.101 12345
   Trying 192.168.56.101...
   telnet: Unable to connect to remote host: Connection refused
   ```

2. 2.抓包分析采用tcpdump抓包保存文件，再采用wireshark分析查看。采用tcpdump抓包时可以指定目标地址或端口，例如：

   ```
   tcpdump -i eth0 port 5060 -s 0 -w example.pcap
   ```

   将生成的pcap文件用wireshark打开，如下图所示，从抓到的INVITE请求中，可以检查对应的国标号、SIP服务器地址和端口、媒体服务器地址和端口（图中蓝色划线部分）。

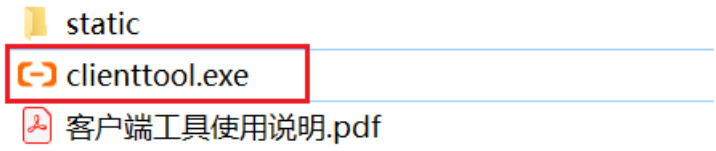


客户端工具

客户端工具Windows版本下载 。

使用说明

- 下载完成后解压到本地，双击clienttool.exe文件即可运行，初始化过程中，页面需要加载，请耐心等待。



- 点击**菜单——>网络**即可实现网络的检测。
- **网络**检测通过，点击**菜单——>摄像头——>默认——>起流**，即可模拟摄像头国标接入的信令注册以及推流实现。
- 具体使用细节请参照 **客户端工具使用说明.pdf** 。

OBS推流功能使用说明

请参见文档OBS推流工具。

9.万网/阿里云解析与配置CNAME流程

您在空间中添加自己的域名后，阿里云视图计算产品会给您分配对应的CNAME地址。如果您想启用推流或播流域名的CDN加速服务，需要将加速域名指向CNAME地址。这样访问加速域名的请求才能转发到CDN节点上，达到加速效果。本文档以您的域名在阿里云解析（原万网）为例。

操作步骤

1. 在**空间管理**页面的空间列表中选中您的空间，点击**空间配置**。
2. 选择**播放域名**，点击**域名配置**。
3. 在域名**基本配置页面**中，点击**复制**，复制CNAME值。
4. 添加CNAME记录 。
   i. 登录域名解析控制台。
   ii. 在域名列表中找到您加速域名对应的主域名，进入**解析设置**页。

iii. 单击**添加解析**，添加CNAME记录。

- 记录类型请选择为CNAME。
- 主机记录即加速域名的前缀，例如：

如果您的加速域名为...	主机录为...
testcdn.aliyun.com	testcdn
www.aliyun.com	www
aliyun.com	@
*.aliyun.com	*

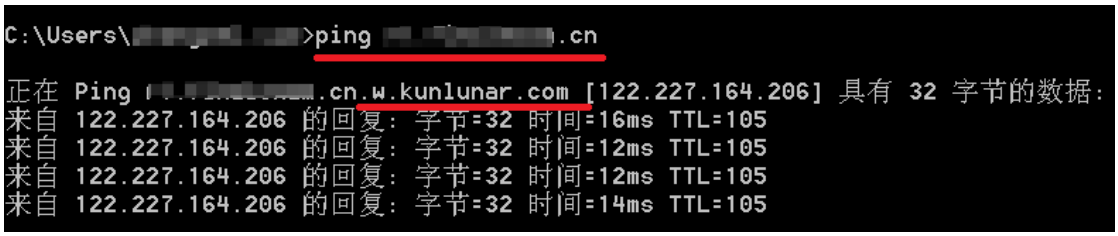
- 记录值填写为步骤1复制的CNAME值。
- 解析线路和TTL保持默认值即可。

iv. 单击 确认，配置CNAME完毕。CNAME配置生效后，视图计算域名配置也会立即生效。

> 说明
>
> - CNAME配置生效时间：新增CNAME记录会实时生效，而修改CNAME记录需要最多72小时生效时间。
> - 添加时如遇添加冲突，可考虑换一个加速域名，或参考解析记录互斥规则自行调整冲突的记录。
> - 配置完CNAME后，由于状态更新约有10分钟延迟，阿里云视图计算控制台的域名列表页可能仍提示未配置CNAME，请忽略。

如何验证CNAME配置是否已生效？

配置CNAME后，不同的DNS服务商CNAME配置生效的时间也不同。您可以 ping或 dig您所添加的加速域名，如果被转向 .kunlun*.com，即表示CNAME配置已经生效，CDN功能也已生效。



此外，您还可以参考DNSPod配置的方法解析。

10.如何配置IP黑名单

域名支持黑名单规则，添加了黑名单的 IP，表示此 IP 无法访问当前加速域名。

注意事项

IP 黑名单当前支持 IP 网段添加，例如：127.0.0.1/24。

其中，24表示采用子网掩码中的前24位为有效位，即用32-24=8bit来表示主机号，该子网可以容纳28- 2 = 254 台主机。故127.0.0.1/24 表示 IP 网段范围是：127.0.0.1~127.0.0.255。

操作步骤

1. 登录视图计算控制台。
2. 单击**空间管理**，选择所需的空间，并单击**空间配置**。
3. 选择 所需的播放域名，单击**域名配置**>IP黑名单，并单击**编辑**。
4. 在IP黑名单 中，输入黑名单IP。
5. 单击**确认**IP黑名单配置成功。

11.跨域访问说明

本文为您介绍跨域访问的操作流程。

H5播放flv、m3u8视频的跨域配置

当出现下面错误时，需要启用播放域名允许跨域访问。

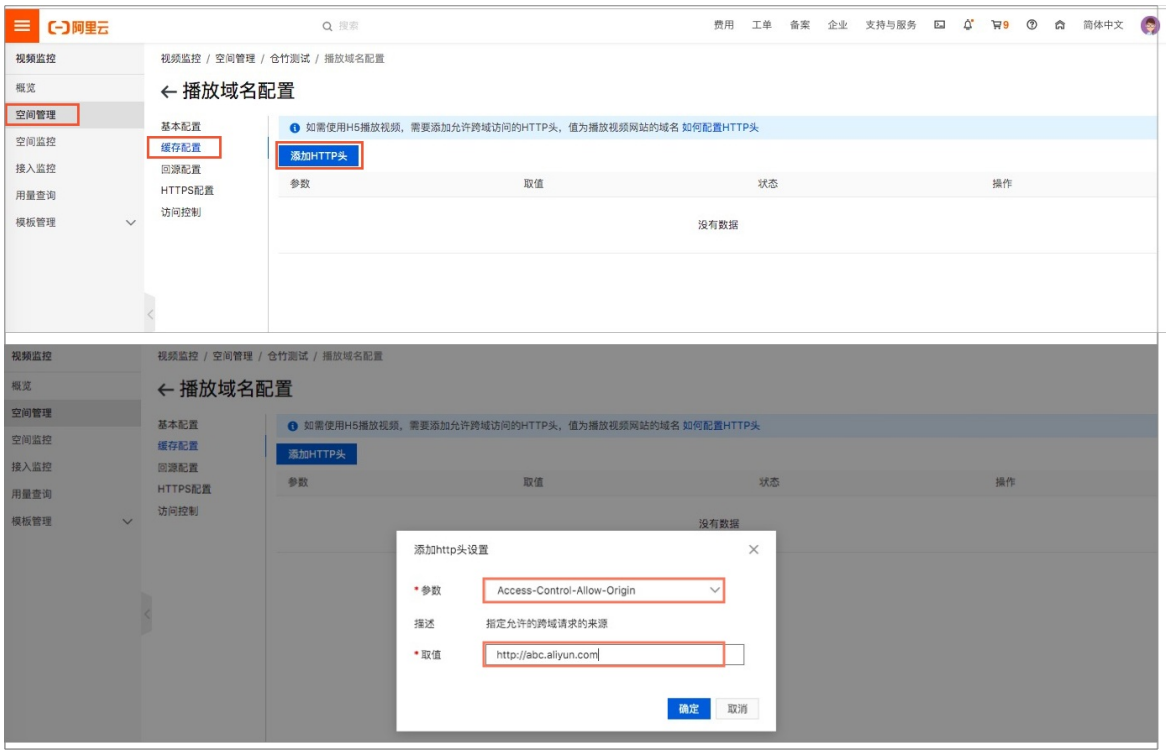
```
No ‘Access-Control-Allow-Origin’ header is present on the requested resource. Origin ‘http://localhost:9030‘ is therefore not allowed access.
```

添加允许跨域访问的header，值为播放视频网站的域名，比如网站为 `https://www.aliyun.com/` ，那么值就为 `https://www.aliyun.com/` 。

- CDN设置跨域访问。
- HTTP访问控制CORS详解。

设置跨域访问。

1. 登录视图计算控制台。
2. 通过空间管理访问具体空间，点击**空间配置**，找到播放域名，点击**域名配置**。
3. 选择**缓存配置**，点击**添加HTTP头**，进行配置。



说明 如果ts分片地址的域名和m3u8的地址的域名不一样，那么ts分片地址的域名也需要添加允许跨域访问的header。

12.NVR注册、国标级联接入流程

你可以通过本文详细了解NVR注册、国标级联接入流程。

NVR设备接入流程

NVR（网络视频存储）设备接入阿里云视图计算过程基本与摄像头接入流程类似，都是需要在阿里云视图计算的空间下先添加设备。然后在设备端进行国标注册操作。注册成功后，阿里云视图计算控制台的**空间监控**的**设备监控**中可以查看接入的NVR设备状态。如果NVR平台上有接入的摄像头，配置的通道信息，在阿里云控制台可以获取到每个接入的通道，可实时预览和回看通道内的监控流，对设备进行启停操作等。

操作步骤说明

1. 在视图计算控制台创建空间，获得空间的接入网关设备IP，端口号和国标ID。

   > **说明** 支持设备通过TCP和UDP两种协议注册，可在摄像头国标注册页面选择TCP或UDP传输协议。同时考虑到网络传输链路上可能存在防火墙对5060等端口进行限制。阿里云视图计算接入网关支持UDP和TCP双协议多端口注册，UDP协议支持端口号5060、5160，TCP协议支持端口号6060、6160。

2. 在视图计算控制台添加NVR设备，填写国标ID，用户名和密码。

   > **说明** 左侧为阿里云监控控制台，右面为NVR设备管理页面示意图。可参看标示进行相应配置。

3. 在NVR设备自身管理页面上，进行平台接入的配置。

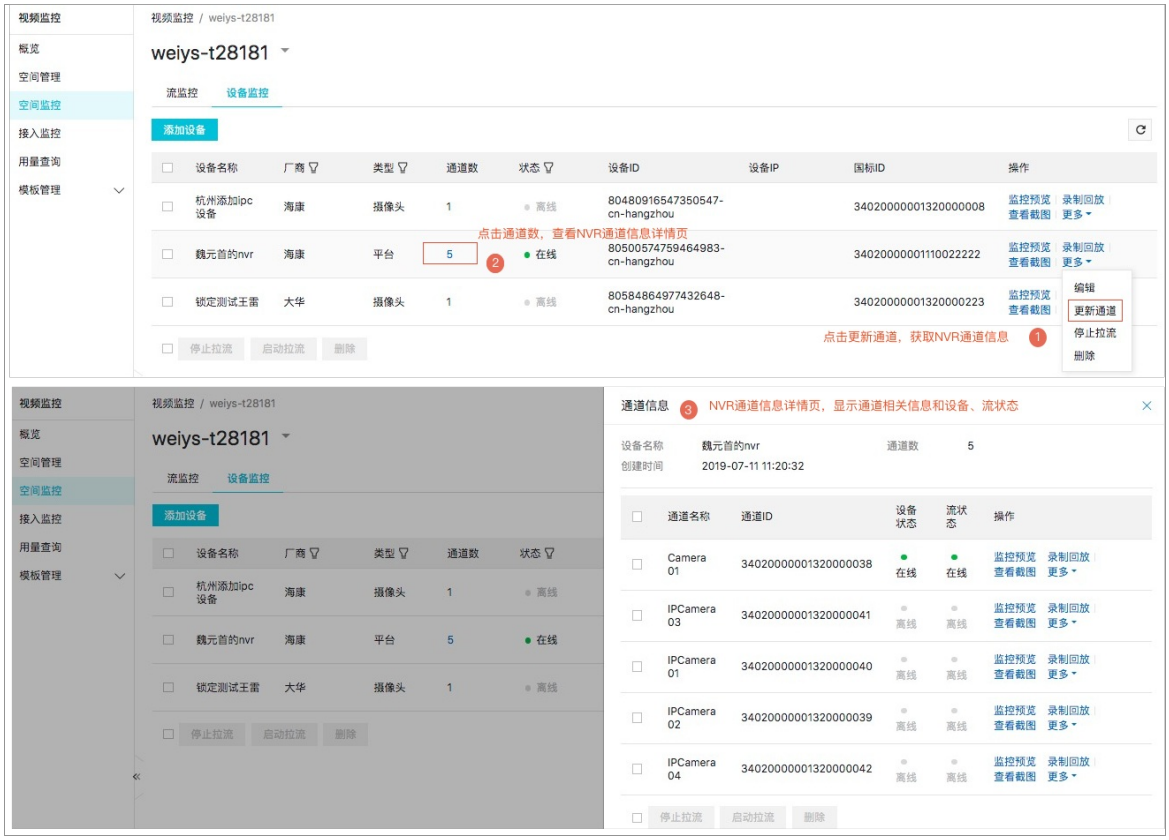
4. IPC接入NVR设备配置。

> **说明** 如果NVR中还没有接入IPC设备，可按照以下步骤把IPC接入NVR，如果摄像头已经在NVR国标注册的通道中进行了配置，可跳过步骤4、步骤5。在NVR中配置IPC可根据设备厂商型号进行相应配置，下图仅示范某厂商设备。

5. 在NVR上配置设备通道，为IPC配置通道编码后，通过获取NVR的通道编码找到对应的IPC设备。

> **说明** 新增IPC到NVR时，添加通道，NVR注册到阿里云可以不设置通道，后面再设备通道。

6. 在视图计算控制台查看NVR和上面配置的IPC信息。



说明 为防止网络影响通道信息获取，建议刷新几次“更新通道”保证获取的通道信息完整。

国标级联

阿里云视图计算支持下级平台通过国标级联的方式接入。视图计算管理平台和NVR注册流程类似。阿里云视图计算服务作为国标注册的上级，视图计算管理平台做为国标注册的下级向阿里云视图计算接入点进行国标级联。

1. 在阿里云视图计算控制台先添加设备，类型选择“平台”。填写下级视图计算管理平台的国标ID，国标注册用户名和密码。
2. 在下级视图计算管理平台配置国标级联

说明

国标级联协议选择“GB/T28181-2016”

信令网关编码处填写阿里云视图计算接入网关设备国标ID（在空间详情信息中可获取，20位国标ID）

信令网关IP地址处填写阿里云视图计算接入网关IP（在空间详情信息中可获取）

信令网关端口处填写阿里云视图计算接入网关端口号（在空间详情信息中可获取）

开启鉴权

设置鉴权realm（阿里云视图计算接入网关国标ID的前十位）

鉴权登录名处填写要与阿里云视图计算控制台添加设备时填写的国标注册用户名保持一致（建议使用平台的国标ID）

鉴权登录密码处填写要与阿里云视图计算控制台添加设备时填写的国标注册用户密码保持一致

13.设置私有bucket回源

录制存储到用户自己的OSS Bucket下，通过CDN进行加速访问时，加速域名要对回源至该账号下私有bucket进行授权。授权成功并开启授权配置后才能访问私有bucket。 您可以配合使用CDN提供的refer防盗链、鉴权等功能，有效保护您的资源安全。

风险提示

- 授权成功并开启对应域名的私有bucket功能后，该加速域名便可访问您私有bucket内的资源内容。请谨慎决策。若您授权的私有bucket内容不适合作为CDN加速域名的回源内容，请勿授权或开启该功能。
- 若您的网站有攻击风险，请购买高防服务，不要授权或开启私有bucket功能。

操作流程

- 如何开启私有bucket回源授权 。
  i. 进入**空间管理**页面，选择需要设置的空间，在**播放域名**处单击**域名配置**。
  ii. 在**回源配置 > 私有Bucket回源**，单击**立即授权**。

  iii. 单击**同意授权**。

  iv. 授权成功后，为该域名开启私有bucket回源，完成配置 。

- 如何关闭私有bucket回源授权 。

i. 登录RAM控制台，单击**RAM角色管理**。

ii. 删除 AliyunCDNAccessingPrivateOSSRole 授权。

> **注意** 如果您的加速域名正在使用私有bucket作为源站进行回源，不要关闭或删除私有bucket授权。

14.如何配置HTTPS

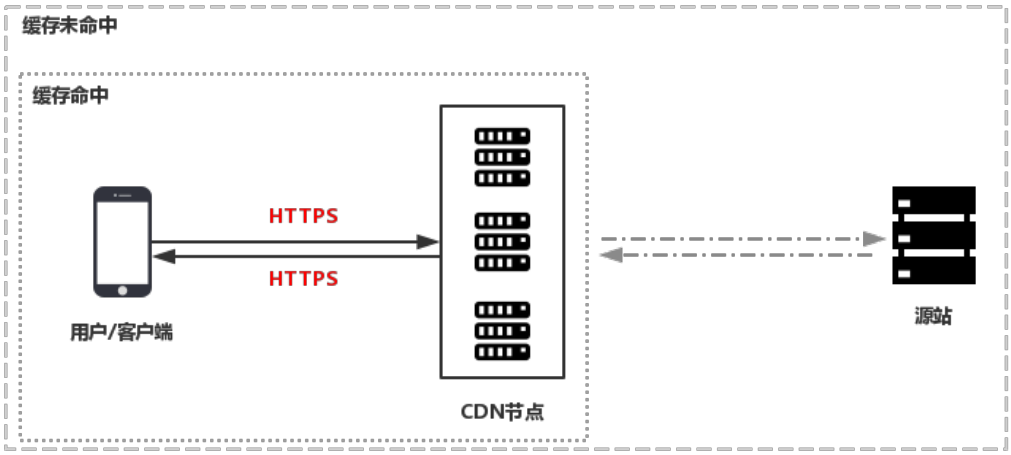
安全超文本传输协议（Hyper Text Transfer Protocol over Secure Socket Layer，简称 HTTPS），是以安全为目标的HTTP通道。简单来说，HTTPS 是 HTTP 的安全版，即将 HTTP 用 SSL/TLS 协议进行封装，HTTPS 的安全基础是 SSL/TLS。

功能优势

传输过程中对用户的关键信息进行加密，防止类似Session ID或者Cookie内容被攻击者捕获造成的敏感信息泄露等安全隐患。 传输过程中对数据进行完整性校验，防止DNS或内容遭第三方劫持、篡改等中间人攻击（MITM）隐患，了解更多使用HTTPS防止流量劫持。 阿里云CDN提供了HTTPS安全加速方案。您只需要开启HTTPS后上传证书和私钥，并支持对证书进行查看、停用、启用、编辑操作。 说明 如果您有SNI回源的需要，请提交工单。

工作原理

在阿里云视图计算控制台开启的HTTPS，将实现用户和阿里云CDN节点之间请求的HTTPS加密。而CDN节点返回源站获取资源的请求仍按您源站配置的方式进行。建议您源站也配置并开启HTTPS，实现全链路的HTTPS加密。 以下是HTTPS加密流程。



1. 客户端发起HTTPS请求。
2. 服务端生成公钥和私钥（可以自己制作，也可以向专业组织申请）。
3. 服务端把相应的公钥证书传送给客户端。
4. 客户端解析证书的正确性。
   - 如果证书正确，则会生成一个随机数（密钥），并用公钥该随机数进行加密，传输给服务端。
   - 如果证书不正确，则SSL握手失败。

   > 说明 正确性包括：证书未过期、发行服务器证书的CA可靠、发行者证书的公钥能够正确解开服务器证书的发行者的数字签名、服务器证书上的域名和服务器的实际域名相匹配。

5. 服务端用之前的私钥进行解密，得到随机数（密钥）。
6. 服务端用密钥对传输的数据进行加密。
7. 客户端用密钥对服务端的加密数据进行解密，拿到相应的数据。

注意事项

配置相关

支持HTTPS安全加速的启用和停用：

启用：您可以修改证书，系统默认兼容用户的HTTP和HTTPS请求。您也可以自定义对原请求方式设置强制跳转。

停用：停用后，系统不再支持HTTPS请求且将不再保留证书或私钥信息。再次开启证书，需要重新上传证书或私钥。

您可以查看证书，但由于私钥信息敏感，不支持私钥查看。请妥善保管证书相关信息。您可以更新证书，但请谨慎操作。更新HTTPS证书后1分钟内全网生效。

计费相关

HTTPS安全加速属于增值服务，开启后将产生HTTPS请求数计费，当前计费标准详见 HTTPS计费详情。

> **说明** HTTPS根据请求数单独计费，费用不包含在视图计算带宽流量内。请确保账户余额充足再开通HTTPS服务，以免因HTTPS服务欠费影响您的服务。

证书相关

- 开启HTTPS安全加速功能的加速域名，您需要上传证书，包含证书和私钥，均为 **PEM** 格式。

  > **说明** 由于视图计算使用的底层CDN采用的Tengine服务基于Nginx，因此只支持Nginx能读取的证书，即 PEM格式)。具体方法，请看参考证书格式说明及转化方法。

- 只支持携带SNI信息的SSL/TLS握手。
- 您上传的证书需要和私钥匹配，否则会校验出错。
- 不支持带密码的私钥。

操作步骤

1. 购买证书。您需要具备匹配加速域名的证书才能开启HTTPS安全加速。您可以在 云盾控制台 快速申请免费的证书或购买高级证书。
2. 登录视图计算控制台，进入 **空间管理**，选择空间，查看域名，选择 **播放域名**，点击 **域名配置**。
3. 选择 **HTTPS设置** > **HTTPS证书**，单击**修改配置**。
4. 在**HTTPS设置**对话框中，开启HTTPS证书。
5. 选择证书。您可以选择的证书类型包括：云盾、自定义和免费证书。目前仅支持 PEM 的证书格式。请参考证书格式说明。
   - 您可以选择云盾。若证书列表中无当前适配的证书，您可以选择自定义上传。您需要在设置证书名称后，上传证书内容和私钥，该证书将会在阿里云云盾的证书服务中保存。您可以在我的证书里查看。
   - 您也可以选择免费证书，即阿里云的Digicert免费型DV版SSL证书。CDN的免费证书的只适用于CDN的HTTP安全加速业务，因此您无法在阿里云云盾控制台管理该证书，也无法查看到公钥和私钥。设置免费证书后，大约需要等候10分钟生效。
6. 验证证书是否生效。证书生效后（约1分钟），使用HTTPS方式访问资源。如果浏览器中出现绿色HTTPS标识，表明当前与网站建立的是私密连接，HTTPS安全加速生效。

   > **说明** 关于更换证书说明：

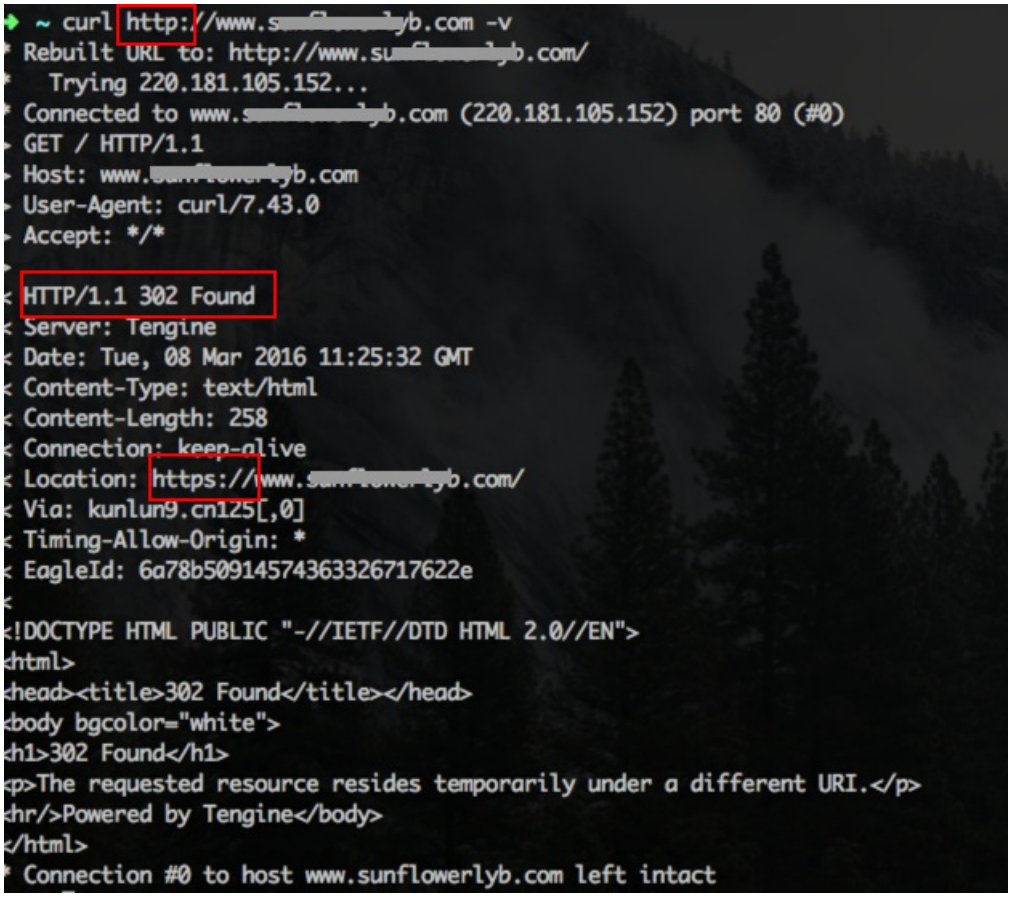
7. 如果您想更换为免费证书或阿里云云盾证书，直接在HTTPS设置页选择想替换的目标证书类型（即云盾或免费证书）即可。
8. 如果您想更换为自定义证书，在HTTPS设置页，选择自定义，然后将新证书的名称和内容填入对应框内，提交信息即可。

15.如何配置强制跳转

您可以通过本文了解配置强制跳转的操作步骤。

功能介绍

如果您的域名开启了HTTPS安全加速，您可以自定义设置，将终端用户的原请求方式进行强制跳转。 例如，当您开启强制HTTPS跳转后，终端用户发起了一个HTTP请求，服务端返回302重定向响应，原来的HTTP请求强制重定向为HTTPS请求，如图所示：



强制跳转默认不开启。开启后默认设置为：同时支持HTTP和HTTPS方式的请求。

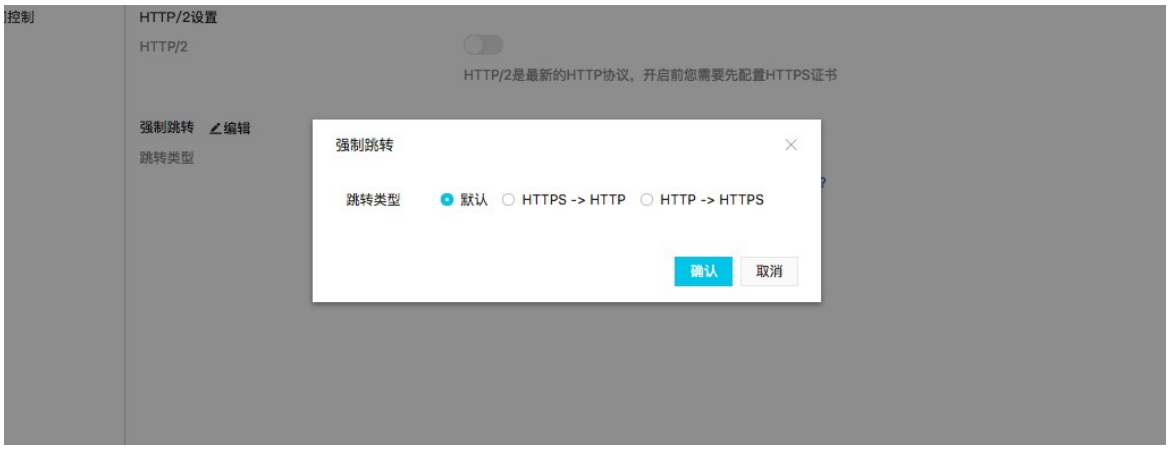
可选项分别是： **默认**、 **强制HTTPS跳转**、 **强制HTTP跳转**。 强制HTTPS跳转：用户的请求将强制重定向为HTTPS请求。 强制HTTP跳转：用户的请求将强制重定向为HTTP请求。

> **说明** 您只有在启用 HTTPS安全功能后才能设置强制跳转。同时支持HTTP和HTTPS方式的请求。

操作步骤

1. 进行域名的HTTPS安全配置。
2. 进行强制跳转设置。


视频监控
概览
空间管理
空间监控
接入监控
用量查询
模板管理
视频监控 / 空间管理 / 上海门店监控 / 播放域名配置
播放域名配置
基本配置
缓存配置
HTTPS配置
访问控制
HTTPS证书 编辑
HTTPS证书
已关闭
1
HTTP/2设置
HTTP/2
HTTP/2是最新的HTTP协议，开启前您需要先配置HTTPS证书
强制跳转 编辑
跳转类型
默认
用户的请求将强制重定向为HTTPS请求 如何配置强制跳转?
2


控制
HTTP/2设置
HTTP/2
HTTP/2是最新的HTTP协议，开启前您需要先配置HTTPS证书
强制跳转 编辑
跳转类型
强制跳转
跳转类型
默认
HTTPS -> HTTP
HTTP -> HTTPS
确认
取消

16.如何设置录制回调

视图计算录制新状态回调，录制完成后会通知用户相应的结果以及录制状态。

注意事项

支持配置HTTP/HTTPS URL，向用户服务器发送POST请求、消息体JSON格式，将录制结果和状态信息实时反馈给用户，用户服务器通过200响应返回接口返回结果。URL无需标识，能正常访问即可。如果访问超时，可以重试5次，每次重试的间隔时间为随机值，范围在100ms到10s之间。

操作步骤

您可以在控制台自主配置录制回调地址。

1. 登录**视图计算控制台**。
2. 单击导航栏的**模版管理**，单击**录制模版**。
3. 在**录制模版**页，点击**添加录制模版**。
4. 在**录制模版详情页**的**录制回调地址** 处填写，完成后单击**创建**。

> **说明** 由于安全原因，录制回调不可以回调内网地址。必须为一个有效的公网地址。 示例 用户回调地址：http:// 1.1.1.1/notify/record返回的body内容如下。

文件生成事件回调示例。

表示目标录制文件已经生成。

```
{
 "domain": "live.aliyunlive.com",
 "app": "live",
 "stream": "hello",
 "uri": "live/hello/0_2017-03-08-23:09:46_2017-03-08-23:10:40.flv",
 "duration": 69.403,
 "start_time": 1488985786,
 "stop_time": 1488985840
}
```

其中domain、app、stream分别为空间的域名、live和流名，uri为目标录制文件在用户录制OSS Bucket下的路径。duration、start_time、stop_time分别为目标录制文件录制内容时长和起止时间。

录制状态回调示例（当 NeedStatusNotify=true 时产生） 录制开始事件回调，表示录制已经成功开始。

```
{
"domain": "live.aliyunlive.com",
"app": "live",
"stream": "hello",
"event": "record_started"
}
```

其中domain、app、stream 分别为录制域名、应用名和流名，event为事件名，可以为record_started/record_paused/record_resumed。

录制暂停事件回调，表示录制已经成功暂停。

```
{
"domain": "live.aliyunlive.com",
"app": "gs_app",
"stream": "gs_stream",
"event": "record_paused"
}
```

录制错误事件回调，表示录制出现错误信息。

```
{
"domain": "gs_domain",
"app": "gs_app",
"stream": "gs_stream",
"event": "record_error"
}
```

17.证书格式说明

开启HTTPS服务前需要配置证书。您可选择云盾证书上的免费证书、购买高级证书或上传自定义证书。自定义上传只支持PEM格式。

证书格式要求

CA 机构提供的证书一般包括以下几种。其中阿里云CDN使用的是 Nginx （.crt为证书，.key为私钥）：

说明 如果证书是通过 root CA机构颁发，则您的证书为唯一的一份。如果证书是通过中级CA机构颁发的证书，则您的证书文件包含多份证书，需要手工将服务器证书与中间证书拼接后，一起上传。 说明拼接规则为：服务器证书放第一份，中间证书放第二份，中间无空行。一般情况下，机构颁发证书时会有对应说明。请确认格式正确后上传。

Linux环境下证书的 PEM 格式为：

```
-----BEGIN CERTIFICATE-----
MIIE+TCCA+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCB
tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSoAYykwOTEvMC0GA1UEAxMm
VmVyaVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzIwHhcNMTAxMDA4
MDAwMDAwWhcNMTMxMDA3MjM1OTU5WjBqMQswCQYDVQQGEwJVUzETMBEGA1UECBMK
V2FzaGluZ3RvbjEQMA4GA1UEBxQHU2VhdHRsZTEYMBYGA1UEChQPQW1hem9uLmNv
bSBJbmMuMRowGAYDVQQDFBFpYW0uYW1hem9uYXdzLmNvbTCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEA3Xb0EGea2dB8QGEUwLcEpwvGawEkUdLZmGL1rQJZdeeN
3vaF+ZTm8Qw5Adk2Gr/RwYXtpx04xvQXmNm+9YmksHmCZdruCrW1eN/P9wBfqMMZ
X964CjVov3NrF5AuxU8jgtw0yu//C3hWnOuIVGdg76626ggOoJSaj48R2n0MnVcC
AwEAAaOCAdEwggHNMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEUGA1UdHwQ+MDww
OqA4oDaGNGh0dHA6Ly9TVlJTZWN1cmUtRzItY3JsLnZlcmlzaWduLmNvbS9TVlJT
ZWN1cmVHMi5jcmwwRAYDVR0gBD0wOzA5BgtghkgBhvhFAQcXAzAqMCgGCCsGAQUF
BwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMB0GA1UdJQQWMBQGCCsG
AQUFBwMBBggrBgEFBQcDAjAfBgNVHSMEGDAWgBSl7wsRzsBBA6NKZZBIshzgVy19
RzB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlz
aWduLmNvbTBABggrBgEFBQcwAoY0aHR0cDovL1NWUlNlY3VyZS1HMi1haWEudmVy
aXNpZ24uY29tL1NWUlNlY3VyZUcyLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFow
WDBWFglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEF
GDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZI
hvcNAQEFBQADggEBALpFBXeG782QsTtGwEE9zBcVCuKjrsl3dWK1dFiq3OP4y/Bi
ZBYEywBt8zNuYFUE25Ub/zmvmpe7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mksr3IQ
3gaE1aN2BSUIHxGLn9N4F09hYwwbeEZaCxfgBiLdEIodNwzcvGJ+2LlDWGJOGrNI
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn
1qiwRk450mCOnqH4ly4P4lXo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELT0e5Y
R7CKx7fc5xRaeQdyGj/dJevm9BF/mSdnclS5vas=
-----END CERTIFICATE-----
```

证书规则为：

请将开头 `———BEGIN CERTIFICATE———` 和结尾 `———END CERTIFICATE———一` 并上传；每行64字符，最后一行不超过64字符。中级机构颁发的证书链：

```
`———BEGIN CERTIFICATE———
———END CERTIFICATE———
———BEGIN CERTIFICATE———
———END CERTIFICATE———
———BEGIN CERTIFICATE———
`———END CERTIFICATE———-``
```

证书链规则：

证书之间不能有空行。每一份证书须符合证书格式说明。

RSA私钥格式要求

rsa私钥规则：

本地生成私钥：`openssl genrsa -out privateKey.pem 2048`，其中privateKey.pem为您的私钥文件。`——-BEGIN RSA PRIVATE KEY——-` 开头，`——-END RSA PRIVATE KEY——-` 结尾；请将这些内容一并上传。

每行64字符，最后一行长度可以不足64字符。

如果您并未按照上述方案生成私钥，得到以下格式的私钥，

`——-BEGIN PRIVATE KEY——-` `——-END PRIVATE KEY——-`

您可以按以下方式转换：

`openssl rsa -in old_server_key.pem -out new_server_key.pem` 然后将new_server_key.pem的内容与证书一起上传。

证书格式转换方式

CDN HTTPS安全加速只支持 PEM 格式的证书，其他格式的证书需要转换成 PEM 格式，建议通过openssl 工具进行转换。以下为几种常用的证书格式转换为 PEM 格式的方法。

DER 转换为 PEM

DER格式一般出现在java平台中。证书转化：`openssl x509 -inform der -in certificate.cer -out certificate.pem`

私钥转化：`openssl rsa -inform DER -outform pem -in privatekey.der -out privatekey.pem`

P7B 转换为 PEM

P7B格式一般出现在windows server和tomcat中。证书转化：`openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer`

获取outcertificat.cer里面 `——-BEGIN CERTIFICATE——-`，`——-END CERTIFICATE——-` 的内容作为证书上传。

私钥转化：P7B证书无私钥，因此，只需在CDN控制台只需填写证书部分，私钥无需填写。PFX 转换为 PEM:

PFX格式一般出现在windows server中。证书转化：

```
openssl pkcs12 -in certname.pfx -nokeys -out cert.pem
```

私钥转化：

```
openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes
```

免费证书

免费证书申请需要5-10分钟。等待期间，您也可以重新选择上传自定义证书或者托管证书。无论您启用的是自定义证书/托管证书，还是免费证书，都可以相互切换。免费证书有效期为1年，到期后自动续签。在您使用过程中，如果关闭Https设置后，再次开启使用免费证书时，会直接使用已经申请过但未过期的证书。若开启时证书已过期，会重新申请免费证书。

其他证书相关

您可以停用、启用和修改证书。停用证书后，系统将不再保留证书信息。再次开启证书时，需要重新上传证书或私钥。只支持带SNI信息的SSL/TLS。请确保上传的证书和私钥匹配。更新证书的生效时间为10分钟。不支持带密码的私钥。

18.视图计算最佳实践

视图计算具体操作步骤指导

https://www.aliyun.com/acts/best-practice/preview?id=52110

19.AUVSP协议接入

本文档介绍AUVSP协议接入流程。

协议介绍

- AUVSP是阿里云视图计算和宇视科技联合共创视频云联网协议，支持免注册“一键上云”、多码流拉取、报警图传等功能，方便设备接入，降低整体成本，仅支持宇视摄像头。

使用限制

- 接入设备
  - 空间选择AUVSP协议仅支持宇视和阿里云合作的一键上云摄像头，包括阿里云UA型号和宇视分销及通用产品，不包括TIC/HIC/EXC行业产品。如果您对那些设备支持仍不了解或想咨询购买宇视-阿里云合作摄像头，请提交工单咨询。
- 现阶段支持AUVSP接入流程需要进行初始化，请提交工单我们支持。

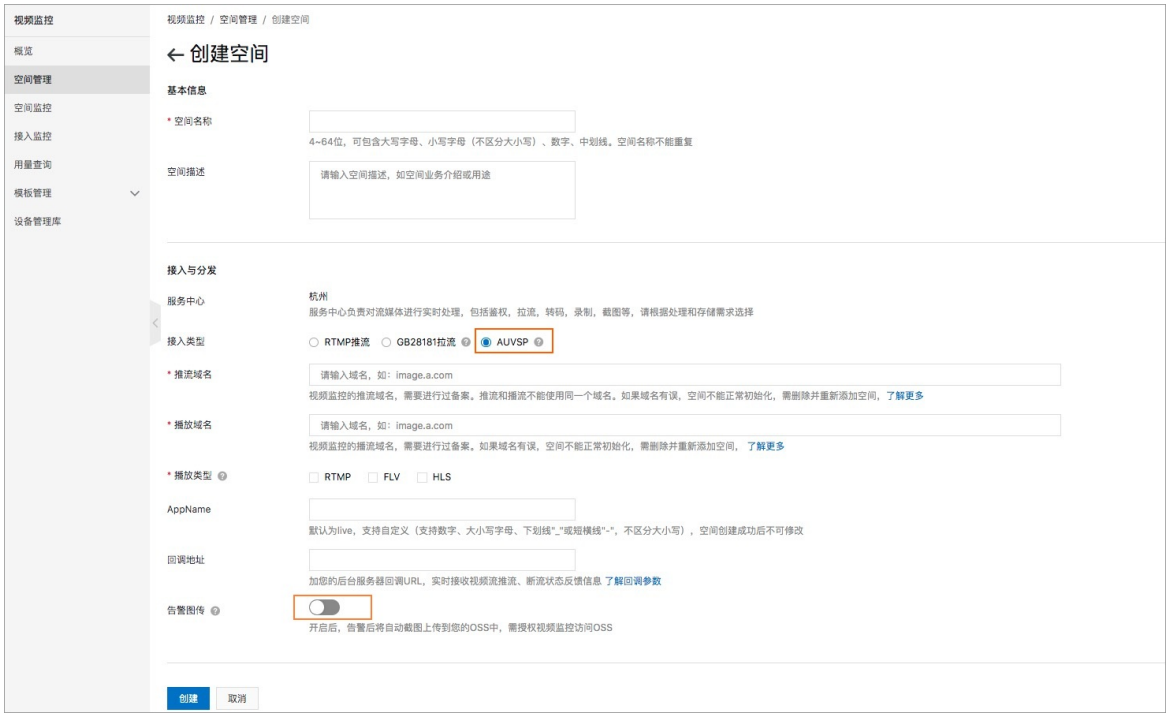
使用前提

- 创建空间需要AUVSP协议需要使用备案过的推流域名和播放域名，请先将域名备案。

操作步骤

1. 登录视图计算控制台，单击**空间管理**。
2. 在**空间管理**页面，单击**创建空间**。

3. 在**创建空间**页面，选择 **AUVSP** 协议类型，配置推流、播放域名，设置基本信息和接入分发信息。



4. 配置按需拉流，如果在空间级别配置开启“按需拉流“。开启后，当有播放/录制/截图时才开始拉流，播放结束后60秒自动停止拉流，对本空间内所有设备生效。特别提示：如果启动按需拉流，请不要同时使用普通录制、时移录制、覆盖截图、实时截图，以上方式的录制、截图都是周期性行为，会导致一直有拉流产生。按需的场景如果需要使用截图和录制功能，请配置按需录制和按需截图。
5. 配置回调通知，添加您的后台服务器回调URL，可实时接收设备在线/离线状态、流启/停状态、告警/告警图传反馈信息。
6. 告警图传是与前端摄像头告警配合进行图片上传云端存储的功能，在前端摄像头进行画面动态变化检测、绊线检测等报警设置，当报警发生后，会按照设置的报警频率把图片上传到您设置的OSS Bucket中，当摄像头报警停止后不再上传图片。报警和每次上传截图成功消息将通过空间回调地址通知。如果开启 **告警图传** 需要配置图片上传存储使用的OSS Bucket。同时要设置图传频率，图传频率是指当摄像头发生报警后上传图片到OSS Bucket的上传频率，范围1-86400秒，默认10秒。

说明：告警是指摄像头上面的动帧检测、绊线检测、区域进入/移出检测，是普通摄像头具备的检测能力，除了含结构化数据告警不支持，其他都支持。具体能力要看摄像头型号，识别那些告警和告警阈值需要在摄像头侧进行设置。

7. 单击**创建**。
8. 空间创建后，可在**空间管理**页面查看空间信息和状态，在**操作**区域，可单击**空间配置**，查看详细配置信息。
9. 在**空间管理**页面的**操作**区域，单击**停用**、**删除**、**启用**，对空间进行停用、删除和启用操作。


视频监控
概览
空间管理
空间监控
接入监控
用量查询
模板管理
视频监控 / 空间管理
空间管理
空间是一个监控业务类型的集合，可对空间下设备和视频流进行统一的管理和配置。最多可有 120个 空间， 当前已有空间4个，还能再创建116个。
创建空间
请输入空间名称
空间ID/名称
空间状态
接入类型
监控中心
设备数量
创建时间
操作
3238675452685107 3
上海门店监控
已启用
RTMP推流
华东2
--
2019-03-01 00:53:24
空间配置 空间监控 停用 删除
3238848773909299 4
高速公路监控
已启用
GB28181拉流
华东2
3
2019-03-01 01:00:17
空间配置 空间监控 停用 删除
3240974443401625 7
社区生活监控
已启用
GB28181拉流
华东2
--
2019-03-01 02:24:45
空间配置 空间监控 停用 删除
3271542340951654 5
明厨亮灶监控
已启用
RTMP推流
华东2
--
2019-03-01 22:39:24
空间配置 空间监控 停用 删除