# HTTP 监听接收事件集成流程

## 1 概述

监听报警是指平台不主动发起连接设备,只是在设定的端口上监听接收设备 主动上传的报警信息(车牌抓拍、人脸比对、门禁主机报警事件等),HTTP监 听是指设备和平台通过HTTP协议上传报警事件,报警数据通过JSON或者XML 文本方式推送到设定的端口中,平台端接收到报警事件的报文后解析。HTTP监 听功能需要设备支持,集成前需要先确认对接设备是否支持此项功能。HTTP监 听过程如下图所示,下文详细介绍HTTP监听的对接流程。



## 2 远程主机配置

使用 HTTP 监听接收设备上传的报警事件首先需要在设备中设置远程主机 的 IP 和端口,设置远程主机的地址告诉设备报警事件触发后往哪里推送,这个 IP 地址也就是平台服务器的地址。服务器部署在局域网内,远程主机的 IP 就是 局域网内服务器的 IP 地址,端口选择一个未被占用的端口。如果服务器部署在 公网上,远程主机的 IP 需要设定为服务器的公网 IP 地址。远程主机的配置一般 可以通过的设备的网页后台进行配置,有的设备没有网页后台或者网页中没有这 个配置选项,那就需要通过协议命令去配置。两种方式说明如下:

## 2.1 WEB 端配置远程主机

登录 Web 管理后台:

- ▶ 设置电脑IP 地址和设备IP 地址在同一网段(例如192.168.1.100)。
- ▶ 在浏览器地址栏输入设备默认 IP 地址,例如 http://192.168.1.64,回 车。

- ▶ 输入用户名和密码。
- ▶ 单击确定。
- 配置远程主机:

不同版本的设备配置方式不同, 交通设备是通过配置 ANPR 参数进行设 置,过程如下:

- ▶ 单击配置一设备配置一系统设置一网口参数
- ▶ 根据实际情况设置 ANPR IP 和端口
- ▶ 设置完成后点击保存

门禁设备是通过配置 HTTP 监听参数,过程如下:

- ▶ 单击**配置—网络—高级配置—HTTP 监听**
- ▶ 根据实际情况设置 IP、端口、URL、协议类型 (http 或者 https),

▶ 设置完成后点击保存

实时收图	图片	日志	配置	💄 admin   🛶 注 销
设备状态 本地配置	设备信息	串口参数 网口	1 DDNS HTTPS 时间设置 28181 服务 EHON	ИE
设备配置	网卡参数	如置		
系统维护	网卡类型	2	10M/100M/1000M自适应 V	
系统设置	自动	検取		
安拉器加	设备IPv	attestile	172 31 156 104	
应用模式	10,475	7/#17	255 255 255 0	
抓拍参数	1643-6	57#3F	255.255.255.0	
图像参数	IPv4默i	网关	172.31.156.1	
出入口	IPv6模式	C	自动获取 🗸	
用户管理	设备IPvi	5地址		
	IPv6默认	网关		
	IPv6子原	陸四		
	物理地坦	Ł	98:df:82:03:06:ef	
	MTU		1500	
	多播地址	Ŀ		
	ANPR IF	e;	172.31.156.12	
	ANPR读	<b>i</b> □:	8090	
	监听主机	UP:	0.0.0.0	
	监听主机	(満口:	7200	
	开启监守	f传图:		
	DNSRE	(学和学		
	DIN SHICK	S NATHLINE		

<b>HIKVISION</b>		预览	人员管理	事件查询	2置			👤 adm
📮 本地		平台接入 ΗΠ	P监听					
日 系统	~	重素						
🖨 网络	^	序号	目的IP或城名		URL	第日	协议类型	
基本配置		1	10.17.35.23		/test	7661	EHome	×
高级配置		2	0.0.0.0		/test	 0	HTTP	
口 视音频								
2. 図像		保存	Ŧ					
📋 计划配置	~							
🚽 对讲配置								
▲ 门禁配置								
♀ 智能配置								

# 2.1 ISAPI 协议命令配置远程主机

如果设备支持 HTTP 监听, Web 后台没有选项进行配置, 那就需要通过协议 命令进行配置。配置工具可以选用 Postman 或者海康官网设备网络 SDK 开发包 中的 ClientDemo 工具调用透传接口进行配置。

操作名称	获取监听主机配置参数
方法类型	GET
	/ISAPI/Event/notification/httpHosts(XML 报文返回)
URL	或者/ISAPI/Event/notification/httpHosts?format=json(json 报文返回,有的设备不
	支持,测试中两种 URL 都测试)
输出参数	见附件《 <u>配置远程主机参数报文</u> 》(提供 JSON 报文)

表 1	获取监听主机配置参数	
11 1	MMM L/MULD X	

表 2	修改全部 HTTP	报警主机配置
12 4		

操作名称	修改全部 HTTP 报警主机配置
方法类型	PUT
	/ISAPI/Event/notification/httpHosts(XML 报文返回)
URL	或者/ISAPI/Event/notification/httpHosts?format=json(json 报文返回,有的设备不
	支持,测试中两种 URL 都测试)
输入参数	见附件《 <u>配置远程主机参数报文</u> 》(提供 JSON 报文)

*说明*:实际配置过程中,先调用 GET 接口获取远程主机配置参数的报文, 然后修改其中节点参数,将修改后的报文作为输入,调用 PUT 操作命令,修改 远程主机的参数,实现远程主机的参数配置。

#### Postman 测试:

前提条件: 电脑与设备接入同一网段的局域网内;

Postman 测试方式同样也是先调用 GET 操作,获取输出报文,修改后然后调用 PUT 操作进行配置。Postman 操作说明如下图所示:

▶ 操作类型选择: GET;

▶ 组装 URL: http://设备 IP 地址:80/ISAPI 命令,例如: http://10.17.35.42:8
0/ISAPI/Event/notification/httpHosts,如果设备是使用 https,端口为 443;
▶ 认证方式: ISAPI 协议命令认证方式为摘要认证,Postman 集成了这种认证方式,在认证方式的选项中选择:Digest Auth,输入设备的用户名和密码;
▶ GET 操作命令是没有输入的,所以输入中选择为空;

▶ 设置完成后,点击 SEND,发送请求到设备中,设备接收到请求后,返回 响应,

▶ 修改 GET 操作获取到的配置报文中的 IP、端口、URL 等节点参数,然 后调用 PUT 操作下发此配置参数到设备中,返回 200 OK 代表成功。

▶ 获取HT操作类型选择GET	组装URL :http://	//设备IP地址:80/ISAPI协议
GET + http://10.17.35.42:80/ISAPI/Event/notification/ht	ttpHosts	
Params Authorization • Headers (6) Body Pre-re-	quest Script Tests Settings	
туре	Username	admin
Digest Auth 🔻	Password	
The authorization header will be automatically generated when you send the request. Learn more about authorization		Show Password
By default, Postman w <mark>选择摘要认证</mark> om the received response, add it to the request, and retry it. Do you want to disable this?	▼ ADVANCED These are advanced configuration options.	填入设备的用户名和密码
Yes, disable retrying the request	Realm 🚺	testrealm@example.com
	Nonce 🕕	Nonce
	Algorithm 🕕	MD5
	dob	e.g. auth-int
	Nonce Count 🕕	e.g. 00000001
Body Cookies Headers (9) Test Results		G Status: 200 OK Time: 7 I



## ClientDemo 透传操作:

ClientDemo 工具配置 HTTP 监听的远程主机参数是通过调用 SDK 中透 传接口 NET\_DVR\_STDXMLConfig()接口实现的,工具下载和配置操作方法见链 接中文档: <u>https://one.hikvision.com/#/link/r3pNgoXpTJLM61PyOk7n</u> 提取密码: ISC4

以上操作完成设备端远程主机的配置,平台端接收到上传的报警事件的 报文还需要开启指定端口的监听,使得指定的端口处于监听状态,才能接受到设 备上传的报文,如果是局域网对接,监听的端口和设备端指定的远程主机的端口 一致,如果是公网对接,监听的端口要设置为服务器本地的端口,公网端口和服务器本地端口通过映射,将公网传输的报文推送到服务器监听的本地端口,下发介绍开启监听后,设备推送事件的流程。

# 3 服务器监听接收事件

服务端对指定的端口开启监听,成功开启监听后,可以通过系统命令查看端口监听是否成功,触发设备上对应的事件后,设备会通过 POST 命令往指定的远程主机端口上推送事件报文。交互的过程可以通过在平台端抓包分析。示例抓包报文如下:

Wireshark · 追踪 TCP 流 (tcp.stream	eq 39) · 以太网 (host 10.17.35.42) -	· 🗆
ST /test HTTP/1.1		
ntent-Type: multipart/for	-data; boundary=MIME_boundary	
st: 10.17.35.111:7662		
ntent-length: 88028	设备通过POST /test命令 UBI 早之前配置远程主机下发的	
nnection: Keep-allve		
MTME boundary		
ntent-Disposition: form-d	ta; name="event_log"	
	推送到的目的地址,即设备端设置的远程主机的地址和端口	
ipaddress : "poptNo": 7662	10.17.35.42 ,	
"protocol":	"HTTP"	
"channelID":	1,	
"dateTime":	"2021-06-23T10:17:43+08:00",	
"activePostCount"	1,	
"eventType":	"AccessControllerEvent", automatical and a second second	
"eventState":	"active", ● ● ● 中针 关望子校	
eventUescription	access controller event ,	
"AccessController	actory, years, f	
"device	ame": "Access Controller".	
"majorE	entType": 5,	
"subEve	tType": 75,	
"name":	······,	
"cardRe	derkind": 1,	
"cardke	derNo: 1,	
"employ	olostring": "1"	
"serial	o": 12,	
"userTy	e": "normal",	
"curren	VerifyMode": "cardOrFaceOrFp",	
"curren	Event": false,	
"frontS	rialNo": 11,	
"label"	nicestatus : underineu ;	
"status	alue": 0.	
"mask":	"no",	
"helmet	: "unknown",	
"pictur	sNumber": 1,	
"purePw	VerifyEnable": true 报警图片数据,并不是所有报警都有图片,具体看事件;	类型
J	· · · · · · · · · · · · · · · · · · ·	
MIME_boundary		
ntent-Disposition: form-d	ta; name="Picture"; filename="Picture.jpeg"	
ntent-Type: image/jpeg		
atent-length: 86961		

接收到的报文解析都是具有标准的 http 协议,解析报警报文需要自行实现, 对应事件的 JSON 或者 XML 报文说明可以联系我司对接技术同事获取。如果配 置正常,设备正常触发报警,平台未收到上传的报警事件,首先通过抓包确定设 备是否上传到指定端口,如果抓包中有设备上传事件,平台侧没有接收到报文, 重点排查一下平台接收解析报文代码、端口监听是否被占用和防火墙是否阻挡。 监听机制设备会推送历史事件,刚开启监听后,设备中会将存储的历史事件先上 传。

#### 附件

#### 配置远程主机参数报文:

- {

"requestURL": "test", /\*ro, opt, string, 请求 URL, range:[,]\*/ "statusCode": 1, /\*ro, req, int, 状态码, range:[,], step:, unit:, unitType:\*/ "statusString": "test", /\*ro, req, string, 状态描述, range:[,]\*/ "subStatusCode": "test", /\*ro, req, string, 子状态码, range:[,]\*/ "errorCode": 1, /\*ro, opt, int, 错误码, range:[,], step:, unit:, unitType:, desc:当 statusCode 不为1 时,错误码,与 subStatusCode 对应\*/ "errorMsg": "ok", /\*ro, opt, string, 错误详细信息, range:[,], desc:当 statusCode 不为1时,错误详 细信息,能具体到某一个参数的错\*/ "HttpHostNotification": [ /\*ro, req, array, 报警主机信息列表, subType:object, range:[,]\*/ { "id": "1". /\*ro, req, string, 序号, range:[,], desc:最大长度为 128\*/ "url": "http://10.7.35.19:9000/alarm", /\*ro, opt, string, URL, range:[,]\*/ "protocolType": "HTTP", 议 类 型 , /\*ro. req, enum, 协 subType:string, [HTTP#HTTP,HTTPS#HTTPS], desc:最大长度为 32\*/ "parameterFormatType ": "json", enum, 参数格式类型, subType:string, /\*ro, req. [json#json,XML#XML,querystring#querystring], desc:最大长度为 32\*/ "addressingFormatType": "ipaddress", /\*ro, req, enum, 地址格式类型, subType:string, [ipaddress#IP 地 址,hostname#域名], desc:最大长度为 32\*/ "ipAddress": "ipv4", /\*ro, opt, enum, IP 地址类型, subType:string, [ipv4#ipv4,ipv6#ipv6], desc:最大长度为 32\*/ "ipv6Address": "test", /\*ro, opt, string, ipv6 地址, range:[,], desc:最大长度为 128\*/ "portNo": 7200, /\*ro, opt, int, 报警通信端口号, range:[,], step:, unit:, unitType:\*/ "httpAuthenticationMethod": "MD5digest", /\*ro, req, string, HTTP 认证方法, range:[,], desc:最大长度为 32, MD5digest 或 none(不认证)\*/ "uploadImagesDataType": "URL", /\*ro, opt, string, 上传图片数据类型, range:[,], desc:URL-图片存储 URL(需要支持并且配置云存储), binary-图片二进制数据, 最大长度为 32\*/ "format": "json",

/\*ro, opt, string, 协议交互格式, range:[,]\*/
"eventType": "alarmResult"
/\*ro, req, string, 触发的事件类型, range:[,],
desc:alarmResult-人脸比对报警上报,
captureResult-人脸加拍上报,
HFPD -高频人员检测事件,
behaviorResult-行为分析结果上报,
executeControlResult-车牌布控,
LFPD-低频人员侦测,
AIOP\_Video-AI开放平台视频分析任务结果上报,
string 类型, 最大长度为 64, 多个类型用逗号隔开\*/

}

]
}