本文档旨在帮助用户如何将网控设备接入到百度天工物联网平台。让用户能够快速的将 网控物联网设备投入"使用",即通过云平台与设备进行交互性测试,在此期间了解物接入的 基础概念和业务逻辑,为后续的开发和业务部署工作提供基础。

一、创建项目

在使用物接入服务前,您需要创建一个百度智能云账号,请自行注册和登录。 1、登录<u>百度智能云官网</u>后,导航栏选择"产品服务"->"物联网服务" -> "物接入 IoT Hub",即可开始使用物接入服务。

○ 百度智能云	最新活动	产品 解决方案	云市场	合作与生态	帮助与支持
云基础		Q 请输入;	*品名称		
人工智能		接入与存储		分析与应)	用
智能大数据		(株)(立) 1-1 (1.1)		~~~~	Minueline time
物联网服务	>	物接入 IOT Hut 物解析 IoT Par	ser	物可视 IoT 时序洞察 Io	visualization oT EasyInsight
安全服务		规则引擎 Rule	Engine	位置服务 D	JuMap
企业应用		时序数据库 TSI	DB		

2、新用户在创建项目之前应先创建计费套餐并设定每个月收发消息的额度,系统将根据额度 自动计算每个月的服务费用。每个用户只能创建一个计费套餐,所有项目将共享该套餐的额 度。

① 按照步骤一进入物接入服务页面,点击立即使用进入天工物联网总览页面

🗘 百度智能云	最新活动	产品	解决方案	云市场	合作与生态	帮助与支持
物接入 Io7	F Huk	0				
物接入(IoT Hub)是一	个全托管的云	服务,	帮助建立设备 判 故障药测	与云端之间	到安全可靠的双 ¥⊠₩Z目	向连接
汉设亩自庄,以又序四里	反曲口波知道也	(美、江)	#J, DXP#JX//	137771014		
立即使用	帮助文档 >					



- ③ 在创建套餐页面选择:
 - * 资源类型:物接入
 - * 当前地域: (由上一步选择的地区决定)
 - 用户可根据需要自行选择付费套餐,以下为免费测试套餐选项:
 - * 购买规格:1百万
 - * 购买信息: 1/2/3个月(最长3个月)

《 返回项目列表	创建套餐		
▲本信息 * 资源类型: * 当前地域:	 物換入 物換入(SIM版) ③ 後北-北京 	所选配置 地域: 华北-北京 购买规慎: 1百万条/月 购买时长: 3个月 (ハ倍: ¥ 0.00	清空配置
* 购买规格:	1 5000 10000	下一步	ž
购买信息 * 购买时长:	1个月 2 3 4 5 6 7 8 9 5 2年 3年		Feedba
每月前一百万分	免费、如果超过免费额度,我们将会放取相应费用。		

选择"下一步"进入付费页面,付费成功后,可进入"项目列表"创建项目。

百度智能云	 ♥ 华南 - 广州 Q
品 天工物联网总览	
- 認物接入 ^	物接入简介
概范	物接入(IoT Hub)是一个全托管的云服务,帮助建立设备与云端之间安全可靠的双向连接,以支撑海量设备的数据收集、监控、故障预测等各种物联网场 景。
项目列表	进入项目列表

连接物接入服务需要先创建一个项目,每个项目会为您对应一个接入点 (endpoint)。一个项目表示一个完整的物接入服务。

2、登录物接入控制台页面,点击"创建项目",填写需要创建 IoT Hub 服务的项 目名称、选择项目类型设备型或数据型,并提交即可。通过项目可以将不同项目的 设备进行隔离和管理。免费测试用户可以创建1个设备型项目,99个数据型项目。

♥ 华南 - 广州						Q	工单	消息	帮助文档	企业组织	财务
用量与计费 项目数: 本月账期: 本月籤度:	● 正常 3 介 2019-07-20 10:03:25 ① 1,000,000 条	C		已用: 1,3 剩余: 99 配置升级	238 条 18,762 条 ① 续费	计费赛繁详 用量详情	情			天工物联网卡 日志服务	0
项目列表											
+ 创建项目	0									请输入名称	
项目名称/Endp	oint	类型	描述	ł	地址		创建印	动间	¢	攝作	
< 返回项目列表				创建项	∃						
】 配置信息 当前地域: * 项目名称: 描述:	华商 - 广州 data_test 0-64李符							P /T 地域: 类型:	西配查 华南 - 广州 数据型	建交	
温馨提示:请 道 项目类型:	全観法理项目失型,送場后智不文特徴	参改。如何选择> 在云號的映像,适用 建工具,快速建立以做 方,无缝对接时序数据 去。权限、反控及OTA	醫于设备的物狀网场景, 影子为核心的物談网应用 講下SDB、物可视等产品 过远程升级等丰富特性	帮助开发者聚							
		皇依赖教戴流的场景, ic,需对协议有较好了 则引拳或自行处理教师	需使用者有较强的软硬作 解 流转及存储	 牛开发能力							

创建项目后,在项目列表页可以看到物接入默认提供的三类地址。选择不同的地址,意味着您可以通过不同的方式连接到百度智能云物接入。

项目名称/Endpoint	类型	描述	地址
m2a	设备型	<u>/</u>	tcp:// ;.mqtt.iot.gz.baidubce.com:1883 ssl://* 3.mqtt.iot.gz.baidubce.com:1884 wss://f 3.mqtt.iot.gz.baidubce.com:443
data_test	数据型	2	tcp:// .jj.mqtt.iot.gz.baidubce.com:1883 ssl:// .jj.mqtt.iot.gz.baidubce.com:1884 wss:// 『jj.mqtt.iot.gz.baidubce.com:443

tcp://yourendpoint.mqtt.iot.gz.baiduce.com:1883,端口1883,不支持传输数据加密,可以通过 MQTT.fx 客户端连接。

ssl://yourendpoint.mqtt.iot.gz.baiduce.com:1884, 端口 1884, 支持 SSL/TLS 加密传输, MQTT.fx 客户端连接,参考配置 MQTT 客户端。

wss://yourendpoint.mqtt.iot.gz.baidubce.com:8884, 端口 8884, 支持 Websockets 方式连接,同样包含 SSL 加密,参考Websockets Client。

物接入提供设备型和数据型两种项目类型。后续步骤中,将分别予以描述,用户请 根据自己期望使用的项目类型,选其一进行了解即可。

后续文档关于 SSL/TLS 方式连接的操作中需多处用到百度天工根证书:

root_cert.pem

请下载后妥善保存,下载地址: https://sdk.bce.baidu.com/console-sdk/root cert.pem

二、设备型项目

步骤一. 获取连接信息

成功创建物接入设备型项目后,点击项目名称,进入项目配置页面。下面以网控物 联网多功能输入输出模块 GNC-NIO 为例,进行创建物模型、物影子和权限组,获取 物接入设备型连接信息,具体操作步骤如下:

项目名称/Endpoint	类型	描述	地址
m2a f0myn83	设备型	2	tcp://f0myn83.mqtt.iot.gz.baidubce.com:1883 ssl://f0myn83.mqtt.iot.gz.baidubce.com:1884 wss://f0myn83.mqtt.iot.gz.baidubce.com:443

1、**创建物模型**: 点击项目名称进入后,选择"物模型",进入物模型列表页面,点击"新建物模型"。

说明: 物模型用来表示一类(或同一型号的一批)设备。可为设备定义一套属性模板,在创建物影子时可以引用该模板,实现业务的快速部署。

	请输入模型名称 Q	
87		Ū m
限组	+	
A远程升级	点击新建物模型	由系统生成,如不需要可以删除。

输入名称、描述,然后添加 GNC-NIO 的全部物模型属性,然后创建。物模型属性说明详见附录 1。

描述: 网控物联网多功能输入输出模块GNC-NIO 模拟量输力: Al1-Al8 开关量输力: D11-D18 进电器输出: DO9-D012 CTA远程升级: COFF 属性: 属性名称 显示名称 类型 散从值 单位 操作 AI1 AI1 number Delet AI1 AI10 number Delet AI2 AI2 number Delet AI3 AI3 number Delet AI3 AI3 number Delet AI3Warn AI3Warn number Delet	名称:	GNC_NIO_Module					
DTA远程升级: CTA远程升级: 属性: 属性: 属性: 属性: A11 AI1 AI1 number Delet A11Warn AI1Warn number Delet A12 AI2 number Delet A12Warn A21Warn number Delet A13 AI3 number Delet A13Warn AI3Warn number Delet A13Warn Delet Delet A13Warn Delet Delet A13Warn Delet Delet A13Warn Dele	描述:	网控物联网多功能输》 模拟量输入:AI1~AI8 开关量输入:DI1~DI8 继电器输出:DO9~D(·輸出模块GNC-NIO D12				
Al1numberDeletAl1WarnAl1WarnnumberDeletAl2Al2numberDeletAl2WarnA21WarnnumberDeletAl3Al3numberDeletAl3WarnAl3WarnnumberDelet	OTA远程升	设: OFF					
AI1WarnAIIWarnnumberDeletAI2AI2numberDeletAI2WarnA21WarnnumberDeletAI3AI3numberDeletAI3WarnAI3WarnnumberDelet	属性:	属性名称	显示名称	类型	默认值	单位	操作
AI2AI2numberDeletAI2WarnA21WarnnumberDeletAI3AI3numberDeletAI3WarnAI3WarnnumberDelet	属性:	属性名称 AI1	显示名称 AI1	类型 number	默认值	单位	操作 Delete
AI2Warn A21Warn number Delet AI3 AI3 number Delet AI3Warn AI3Warn number Delet	属性:	属性名称 AI1 AI1Warn	显示名称 AI1 AI1Warn	类型 number number	默认值	单位	操作 Delete Delete
AI3 AI3 number Delet AI3Warn AI3Warn number Delet	属性:	属性名称 AI1 AI1Warn AI2	显示名称 AI1 AI1Warn AI2	类型 number number number	默认值	单位	操作 Delete Delete Delete
AI3Warn AI3Warn number Delet	層性:	属性名称 AI1 AI1Warn AI2 AI2Warn	显示名称 AI1 AI1Warn AI2 A21Warn	类型 number number number number	默认值	单位	操作 Delete Delete Delete Delete
	扈性:	属性名称 AI1 AI1Warn AI2 AI2Warn AI3	显示名称 AI1 AI1Warn AI2 A21Warn AI3	类型 number number number number number	默认值	单位	操作 Delete Delete Delete Delete Delete

< 创建物模型

2、**创建物影子:** 左侧选择"物影子",进入物影子管理页面,点击"新建物影子"。输入物影子名称,并选择物模型(这里选择上一步创建的GNC_NI0_Model),点击"创建",进入下一步。

* 名称:	Dev_NIO		
描述:	0-128个字符		
* 选择物模型:	GNC_NIO_Module	~	模型详信
存储配置:	OFF		

3、获取连接信息:物影子创建完成后,弹出连接信息,建议下载后妥善保存。



若连接信息未及时保存或密码丢失,亦可点击相应影子的卡片,进入物影子详情页 面,随后通过以下路径查看连接信息或重新生成密钥。

< Dev_NIC)				
物影子详情	物详情 	交互			
名称:		Dev_NIO	编辑	C 刷新	连接配置
描述:					
来自模型:		GNC_NIO_Module			
存储配置:		OFF			

步骤二. 网控物联网设备配置

打开 GNC 设备发现与管理工具,发现认证登陆设备后进入设备物联网配置界面。

勾选启用。保持连接的时间间隔 120 秒,发布数据的超时时间 15 秒。

连接方式: TCP

物联网接入中心类型:百度天工。下方的参数框自动切换到百度智能云设置界面。

服务器域名: yourendpoint.mqtt.iot.gz.baiduce.com

端口号: TCP 方式缺省 1883

项目类型: 设备型项目

项目名: yourendpoint

设备名: 物影子名称

密码:物影子连接信息里的密钥

之后"保存","重启"设备。至此,设备的物联网配置完成。

物联网设置				
读配置	部分产品运	至需要在系统设置当中选择对应的数据上报方式或者协议		
中心MQTT服务	各器1设置 中心MQTT服务	齐器2设置		
☑ 启用		保存		
MQTT协议版本	缺省 ▼ QOS O(almo:	st once) 🗸 保持连接的时间间隔 120 秒 发布数据的超时时间 15 秒		
📃 清除断开期间	目服务器缓存的下发命令(Clean session) 🗌 保持最后发布的内容(Retain),很多云不支持此选项		
□ 启用断开发和	佈信息功能(₩ill),很多云	不支持此选项		
断开信息的。	QOS 0 ▼ 🗌 保持发材	币的断开信息(Will Retain) 断开信息的话题 devices/gnc-nio/mes:		
连接方式 TC	P			
物联网接入中心	5类型 百度天工	•		
百度智能云				
服务器域名	fOmyn83.mqtt.iot.gz.	baidubce.com		
端口号	1883 (TCP缺省	自1883, SSL缺省1884)		
项目类型	设备型项目 ▼			
项目名	·	设备名(设备型物影子名称,数据型-指定的用户名)		
f0myn83		Dev_NIO		
密码	1			
数据型的上报	K话题(一般设device/up)	数据型的控制话题(一般设device/control)		
以上的话题设	贵王要与百度物接入当中的贫	 6略设置一致		

服务器域名、端口号、项目名、设备名和密钥见如图的连接信息。



步骤三. 查看设备运行状态

在项目物影子管理页面,可以看到添加的 GNC-NIO 已显示在线。

Dev_NIO 说明:	● 在线	ė V
属性总计:40	1	
DI1:1	DI1Warn : 2	2
DI2:1	查看更多>	

点击物影子卡片查看影子详情,动作接入到 DI1[~]DI8 的测试开关或改变 AI1[~]AI8 输入的模拟量大小,刷新即可看到各属性的当前值和对应的告警值同步更新。

< Dev_NIO								
物影子详情物详	精 交互							
名称:	Dev_NIO							
描述:								
创建时间:	2020-03-19 17:2	22:38						
最后活跃时间:	2020-03-20 09:	35:23						
物影子版本号:	12							
固件版本号:								
影子状态:	模型数据	原始数据						
								编辑 C 刷新 清空物影子
	属性名称	显示名称	类型	默认值	单位	当前值	修改时间	期望值 发送时间
	AI1	AI1	number			14.27	2020-03-20 09:28:48	N/A
	AI1Warn	AI1Warn	number			1	2020-03-20 09:28:48	N/A
	AI2	AI2	number			0.006	2020-03-20 09:28:48	N/A
	AI2Warn	A21Warn	number			0	2020-03-20 09:28:48	N/A

例如要控制 NIO 的继电器 1[~]4 闭合(DO9[~]DO12),选择"编辑"然后在"期望值" 栏输入"1"("0":断开),点击下方"确定"即可控制继电器动作。

	称	THE PARTY OF THE P	大王	#(#/IE	千位		IN FX HJIHJ	和王坦	2.5NP
	DO9	DO9	numb er			0	2020-03-20 09:35:33	1	2020-03-2 09:40:32
	DO9Wa m	DO9Warn	numb er			D	2020-03-20 09:35:33	输入	N/A
定	取消								

步骤四. SSL/TLS 连接

上述步骤一到三, 演示了网控物联网设备以 TCP 方式连接到百度天工设备型项目, 并进行控制测试。对于安全级别要求较高的场合, TCP 方式便不再适用, 此时需要 通过 SSL/TLS 连接云平台, 以提高数据传输安全性。物模型和物影子的创建过程, 以及连接成功后查看设备运行状态和在线调试等功能对于两种连接方式均相同, 此 处不多赘述。

网控设备的连接到百度天工设备型项目的物联网设置中,SSL/TLS 连接的配置类型 分为两种,对应两个不同的安全级别,由低到高分别为 CA 签名的服务器(不强制 证书检查),CA 签名的服务器(强制证书检查)。

后续配置中服务器域名、端口号、项目名、设备名和密钥见连接信息。

		and a contract
密钥丢失无法找	回,只能在配置	中重新生
t az baidubce o		
az baidubce.co	m:1884	
ot.gz.baidubce.	om:443	
	t.gz.baidubce.co gz.baidubce.co ot.gz.baidubce.o	t.gz.baidubce.com:1883 gz.baidubce.com:1884 ot.gz.baidubce.com:443

1、CA 签名的服务器(不强制证书检查) **连接方式:** SSL **证书类型:** CA 签名的服务器 **端口号:** 1884 保存,重启即可。

 物联网设置 回 X
读配置 部分产品还需要在系统设置当中选择对应的数据上报方式或者协议
中心MQTT服务器1设置 中心MQTT服务器2设置
● 月四 MOTT协议版本 執為 ● OOS D(almost ange) ● 保持连接的时间间隔 120 秒 发布教揮的招时时间 15 秒
□ 启用断开发布信息功能(Will),很多云不支持此选项
断开信息的QOS 0 ▼ □保持发布的断开信息(Will Retain) 断开信息的话题 devices/gnc-nio/mes:
连接方式 SSL ▼
-SSL/TLS连接设置
证书类型 CA签名的服务器(CA signed server certificate) ▼ □ 强制证书检查
下传证书文件
CA:1521字节 设备证书:1585字节 设备密钥:1676字节 证书格式:PEM
物联网接入中心类型
百度智能云
服务器域名 fOmyrn83.mqtt.iot.gz.baidubce.com
端口号 1884 (TCP缺省1883, SSL缺省1884)
项目类型 设备型项目 ▼
项目名 设备名(设备型-物影子名称,数据型-指定的用户名)
f0myn83 Dev_NIO
密码 r i i i i 20
数据型的上报话题(一般设device/up) 数据型的控制话题(一般设device/control)
以上的话题设置要与白度物接入当中的策略设置一致

2、CA 签名的服务器(强制证书检查)

连接方式: SSL

证书类型: CA 签名的服务器

勾选强制证书检查。

下传证书文件: 百度天工根证书《root_cert.pem》

D:\BaiduDeviceCA\Ba	iduRootCA\root_cert.pem
证书格式	

端口号: 1884

保存,重启即可(新下传的证书文件会覆盖旧文件)。

 物联网设置 回 X
读配置 部分产品还需要在系统设置当中选择对应的数据上报方式或者协议
中心MQTT服务器1设置 中心MQTT服务器2设置
◎ 自用
MQTT协议版本 缺省 ▼ QOS 0(almost once) ▼ 保持连接的时间间隔 120 秒 发布数据的超时时间 15 秒
□ 清除断开期间服务器缓存的下发命令(Clean session) □ 保持最后发布的内容(Retain),很多云不支持此选项
□ 启用断开发布信息功能(Will),很多云不支持此选项
助升信息的QOS 0 ▼
注接力式 SSL ▼
SSL/ILS注接反血 江井米刑 Cu终之的昵名哭(Cull aigned carrier certificate) ▼ 回识地计书林本
W 中利亚市協力 W 加利亚市協力
CA:1521字节 设备证书: 1585字节 设备密钥: 1676字节 证书格式: PEM
物联网接入中心类型 百度天工 🔻
百度智能云
服务器域名 fOmyn83.mqtt.iot.gz.baidubce.com
端口号 1884 (TCP缺省1883,SSL缺省1884)
项目类型 设备型项目 ▼
项目名 设备名(设备型-物影子名称,数据型-指定的用户名)
fOmyn83 Dev_NIO
密码 1 1 1 1 2 0
数据型的上报话题(一般设device/up) 数据型的控制话题(一般设device/control)
以上的话题设置要与百度物接入当中的策略设置一致

三、数据型项目

步骤一. 获取连接信息

成功创建物接入数据型项目后,点击项目名称,进入项目配置页面。下面以网控物 联网多功能输入输出模块 GNC-NIO 为例,进行创建用户、身份和策略,获取物接入 连接信息,具体操作步骤如下:

项目名称/Endpoint	类型	描述	地址
data_test wnc8qgj	数据型	2	tcp://wnc8qgj.mqtt.iot.gz.baidubce.com:1883 ssl://wnc8qgj.mqtt.iot.gz.baidubce.com:1884 wss://wnc8qgj.mqtt.iot.gz.baidubce.com:443

1、创建策略: 在项目配置页面选择"策略列表"->"创建策略"。

输入策略名称, 主题(Topic), 选择主题的权限: 发布(Publish)、订阅 (Subscribe)。

创建策略			
* 名称:	device_policy	? 🛛	
* 主题:	device/up	? 🛛	
* 权限:	✓ 发布(PUB) □ 订阅(SUB)		
* 主题:	device/control	? 🔮 😔	
* 权限:	□ 发布(PUB) ✓ 订阅(SUB)		
* 主题:	device/disconnect	? 🔮 😔	
* 权限:	✓ 发布(PUB) □ 订阅(SUB)		
	·		
		确定	取消

(1) 创建**设备端策略"**device_policy"

(2) 创建软件客户端策略 "software_policy"。

创建策略			×
<mark>*</mark> 名称:	software_policy	0 0	
* 主题:	device/up	00	
* 权限:	□ 发布(PUB) ✓ 订阅(SUB)		
<u>*</u> 主题:	device/control	0 0 0	
* 权限:	✓ 发布(PUB) □ 订阅(SUB)		
* 主题:	device/disconnect	000	
* 权限:	□ 发布(PUB) ✓ 订阅(SUB)		
	+ 新增主题		
		确定 取消	

说明:每个策略可以创建多个主题(Topic),点击"+"可以新增更多的主题。

device/up

描述:设备(GNC-NIO)上报数据的主题。由设备端发布,软件客户端订阅。

device/control

描述:为客户端下发给设备控制命令的主题。由软件端发布,设备端订阅。

device/disconnect

描述:遗嘱消息主题。在设备网络连接断开后, IoT Hub 将会自动向该主题发送遗嘱消息。

也可使用自定义主题,如 device/gncnio/up,后续设备的物联网设置的话题和 连接测试的话题需与策略的设置一致。

添加主题时,可以使用"#"或"+"作为通配符,关于通配符的介绍,请参看 关于关于<u>通配符的使用方法</u>。

- 2、创建身份: 在项目配置页面选择"身份列表"->"创建身份"。
- (1) 创建设备端身份
 - ① 输入名称,认证方式选择"密码认证"。

	创建身份 🛛 🗙 🗙	
	 创建身份 > ② 设置策略 > ③ 配置确认 * 名称: device ② ● * 认证方式: ○ 证书认证 ● 密码认证 ③ ● 	
2 策略选	下一步 取消 选择之前创建的设备端策略"device_policy"。	
	初建身份 ス	
	✓ 创建身份 > 2 设置策略 > 3 配置确认	
	* 策略: device_policy Ø	
	为设备选择策略(包括主题和权限),若没有须创建	
	上一步 下一步 取消	
③ 生成长	└────────────────────────────────────	管。
	创建身份 ×	
	⊘ 创建身份 > ⊘ 设置策略 > 3 配置确认	
	身份	
	名称: device	
	密钥: oKLWzuv 点击复制 请合理保管以上密钥,密钥丢失无法找回,只能重新生成	
	策略	
	名称: device_policy	
	确认	

- (2) 创建客户端身份
 - ① 输入名称,认证方式选择"密码认证"。

创强	均分		
	1 创建身份 > (2) 设置策略 > (3) 配	置确认
3	·名称: software	0	0
3	《认证方式: () 证书认证 🤇) 密码认证 🛛 🥥	
		此一才	取消
② 策略选择之	前创建的客户端策	E略 "software_po	olicy"。
创建	身份		
	⊘ 创建身份 >	2 设置策略 > ③ 配	置确认
	策略: software_polic	И	0
đ	り设备选择策略(包括主题和	汉限),若没有须创建	
		上一步下一步	▶ 取消
		2 户 沪 注于 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	主页主伯色
③ 生成 <mark>客户靖</mark>	身份密钥 。用于图	-尸 师 连 按 测 试 ,	阴女普休官
③ 生成 <mark>客户靖</mark> 创题	身份密钥 。用于容 }%	r尸 ^师 连接测试,	旧女告休官
③ 生成 <mark>客户站</mark> 创题	诗身份密钥。用于容 詩份 ○ 创建身份 > (甲女 告 休 目 置确认
3 生成 <mark>客户站</mark> 创题	詩 伊 密 钥 。 用 十 容 詩 份 ○ 创建身份 > (身份	☞ 尸 ' ' 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「 」	吗 女 告 休 目 置确认
3〕生成 <mark>客户站</mark> 创题	身份密钥 。用于容 身份 ③ 创建身份 > (身份 名称: software	▶ 7 师理按测试,	唱 女 苦 休 首 置确认
③ 生成 <mark>客户站</mark> 创题	時身份密钥。用于容 請份 ③ 创建身份 > (身份 名称: software 密钥: 71m □□□□ 请合理保管以上	▶ 戸 端 注 按 测 认 , ✓ 设置策略 > 3 配 ■ XRKh 点击复制 密钥 ,密钥丢失无法找回 ,	旧 女 苦 休 首 置确认 只能重新生成
3〕生成 <mark>客户站</mark> 创题	 ● 身份密钥。用于容 ● 创建身份 > (身份 名称: software 密钥: 71m 一、清合理保管以上 策略 	▶ 尸 端 注 按 测 认 , ✓ 设置策略 > 3 配 ■ XRKh 点击复制 密钥 ,密钥丢失无法找回 ,	旧 女 苦 休 首 置确认 只能重新生成

- 3、创建用户: 在项目配置页面选择"用户列表"->"创建用户"。
- (1) 创建设备端用户
 - ① 输入名称,然后下一步。

	创建用户	×
	1 创建用户 > 2 设置身份 > 3 设置策略 > 4 配置确认	
	* 名称: gnc_nid ? Ø	
	用户名: wnc8qgj/gnc_nio	
	下一步取消	
② 设置身	份选择之前创建的设备端身份"device"。	
	创建用户	×
	✓ 创建用户 > 2 设置身份 > 3 设置策略 > 4 配置确认	
	* 身份:	
	为设备选择安全访问身份,若没有须创建	
	上一步 下一步 取消	
③ 配置确	上—步 下—步 取消	
③ 配置确	上—步 下—步 取消 认。 创建用户	×
③ 配置确	上步 下步 取消	×
③ 配置确	上步 下步 取消 认。 创建用户 ◇ 创建用户 > ◇ 设置身份 > ◇ 设置策略 > ④ 配置确认 设备	×
③ 配置确	上一步 下一步 取消 认。 创建用户 ◇ 创建用户 > ◇ 设置身份 > ◇ 设置策略 > ④ 配置确认 设备 名称: gnc_nio	×
③ 配置确	上一步 下一步 取消 认。 创建用户 ◇ 创建用户 > ◇ 设置身份 > ◇ 设置策略 > ◆ 配置确认 设备 名称: gnc_nio 身份	×
③ 配置确	上→步 下→步 取消 创建用户 ◇ 设置身份 > ◇ 设置策略 > ④ 配置确认 设备 身份	×
③ 配置确	上步 下步 取消	×
③ 配置确	上步 下-步 取消	×

- (1) 创建客户端用户
 - ① 以测试客户端为例,输入名称,然后下一步。

	Cole (D)	^
	 创建用户 > ② 设置身份 > ③ 设置策略 > ④ 配置确认 * 名称: 	
	用户名: wnc8qgj/gncsoft	
	下一步取消	
② 设置身	份选择之前创建的客户端身份"software"。	
	创建用户	×
	✓ 创建用户 > 2 设置身份 > 3 设置策略 > 4 配置确认	
	* 身份: 🛛 🖉	
	为设备选择安全访问身份,若没有须创建	
	上一步 下一步 取消	
③ 配置	→→ 取消 确认。	
③ 配置	止—步 下—步 取消 确认。 创建用户	×
③ 配置	上一步 下一步 取消 确认。 创建用户 ◇ 创建用户 > ◇ 设置身份 > ◇ 设置策略 > ◆ 配置确认	×
③ 配置	上-步 下-步 取消 确认。 创建用户 ◇ 创建用户 > ◇ 设置身份 > ◇ 设置策略 > ④ 配置确认 设备	×
③ 配置	上一步 下一步 取消 确认。 创建用户 ◇ 创建用户 > ◇ 设置身份 > ◇ 设置策略 > ④ 配置确认 设备 名称: gncsoft	×
③ 配置	上一步 下一步 取消 确认。 创建用户 ② 创建用户 > ③ 设置身份 > ④ 设置策略 > ④ 配置确认 设备 名称: gncsoft 身份	×
③ 配置	上一步 下一步 取消 确认。 创建用户 创建用户 > 设备 名称: gncsoft 身份 名称: software	×
③ 配置	上一步 下一步 取消 确认。 创建用户 ② 创建用户 > ③ 设置身份 > ④ 设置策略 > ④ 配置确认 设备 名称: gncsoft 身份 名称: software 策略	×
③ 配置	上一步 下一步 取消 确认。 创建用户 ◇ 创建用户 > ◇ 设置身份 > ◇ 设置策略 > ④ 配置确认 设备 名称: gncsoft 身份 名称: software 策略 名称: software_policy	×

至此,网控物联网设备接入百度天工数据型项目的配置完成,并获得连接信息。

步骤二. 网控物联网设备配置

打开 GNC 设备发现与管理工具,发现并认证登陆设备后点击进入设备物联网配置界面。

勾选启用。保持连接的时间间隔 120 秒,发布数据的超时时间 15 秒。

断开信息的话题: 可选。遗嘱消息主题, device/disconnect

连接方式: TCP

物联网接入中心类型:百度天工。下方的参数框自动切换到百度智能云设置界面。

服务器域名: yourendpoint.mqtt.iot.gz.baiduce.com

端口号: TCP 方式缺省 1883

项目类型:数据型项目

项目名: yourendpoint

设备名: 创建的设备端用户名

密码:为步骤一中,2.1.3 创建 device 身份生成的设备身份密钥

数据型的上报话题: device/up,若使用自定义主题注意与策略保持一致 **数据型的控制话题**: device/control,若使用自定义主题注意与策略保持一致 之后"保存", "重启"设备。至此,设备的物联网配置完成。

读配置	3分产品还需要在系统设置当中选择对应的数据上报方式或者协议
中心MQTT服务器1设置 中心	MQTT服务器2设置
☑ 启田	保存
	S O(almost once)
 □ 清除断开期间服务器缓存的下 □ 启用断开发布信息功能(₩ill 	发命令(Clean session) 🔤 保持最后发布的内容(Retain),很多云不支持此选项),很多云不支持此选项
断开信息的QOS 0 ▼ [【保持发布的断开信息(Will Retain) 断开信息的话题 device/disconnect
连接方式 TCP ▼	
120年7月1日度大 百度智能云 服务器域名 wnc8qgj.mqtt	.iot.gz.baidubce.com
1014KF31技入中心英企 百度智能云 服务器域名 wnc8qgj.mqtt 満口号 1883	⊥ .iot.gz.baidubce.com (TCP缺省1883, SSL缺省1884)
2014773技入中心実望 百度智能云 服务器域名 wnc8qgj.mqtt 端口号 1883 项目类型 数据型项目	⊥▼ .iot.gz.baidubce.com (TCP缺省1883, SSL缺省1884) ▼
120年7月3日本中の英学 百度智能云 服务器域名 wnc8qgj.mqtt 端口号 1883 项目类型 数据型项目 项目名	▲
1214KF31技入中心英望 百度智能云 服务器域名 wnc8qgj.mqtt 端口号 1883 项目类型 数据型项目 项目名 wnc8qgj	▲
1900(F313(ストロの実金) 自慶大 百度智能云 服务器域名 wnc8qgj.mqtt 端口号 1883 项目类型 数据型项目 项目名 wnc8qgj 密码 oF	⊥
10年7月3日大中心失望 日夏大 百度智能云 服务器域名 wnc8qgj.mqtt 端口号 1883 项目类型 数据型项目 项目名 wnc8qgj 密码 or 数据型的上报话题(一般设dev	▲
TakenargA中心突望 百度智能云 服务器域名 wnc8qgj.mqtt 端口号 1883 项目类型 数据型项目 项目名 wnc8qgj 密码 oF 数据型的上报话题(一般设dev device/up	↓ .iot.gz.baidubce.com (TCP缺省1883, SSL缺省1884) ↓ 设备名(设备型-物影子名称,数据型-指定的用户名) gnc_nio uv rice/up) 数据型的控制话题(一般设device/control) device/control

服务器域名和端口号:

项目名称/Endpoint	类型	描述	地址
<mark>data_test</mark> wnc8qgj	数据型	<u>0</u>	tcp://wnc8qgj.mqtt.iot.gz.baidubce.com:1883 ssl://wnc8qgj.mqtt.iot.gz.baidubce.com:1884 wss://wnc8qgj.mqtt.iot.gz.baidubce.com:443
项目名和设备名:			
用户名	描述		创建时间
wnc8qgj/gnc_nio	2		2020-03-18 17:15:36

步骤三. 通过百度天工物接入平台测试

1、在用户列表页面选择"连接测试",可以创建多个用户同时进行连接测试。

wnc8qgj			
+ 创建用户 ⑦			wnc8qgj/ 请输入用户名称
用户名	描述	创建时间	攝作
wnc8qgj/testsoft	<u>e</u>	2019-06-25 09:22:26	连接测试 编辑 删除
wnc8qgj/gncsoft	<u>/</u>	2019-06-24 17:35:08	连接测试编辑删除

注意:进行连接测试的用户须是绑定了 software 身份或对应策略的主题和权限相同。

✓ 创建用	户 > ♥ 设置身份 > ♥ 设置策略	🖒 🍊 配置确认
设备		
名称:	gncsoft	
身份		
名称:	software	
策略		
名称:	software_policy	

2、以 gncsoft 用户为例,进入天工物接入测试页面,身份密码为步骤一中, 2.2.3 创建的 software 客户端身份密钥,点击"connect",提示连接成功。

主机名称:	wnc8qgj.mqtt.iot.gz.baidubce.com 🔮 *端口: 8884 🥌 *用户I	JD : DeviceId-pctqhacx1i
用户名:	wnc8qgj/testsoft • 常易份密钥: · · · · · · · · · · · · · · · · · · ·	Alive : 60 SSL 🖉 💿 Clean Session 🔽
ast-Will Topic :	请输入Last-Will Topic Last-V	Mill QoS : 0 ♥ Last-Will Retain ♥
ist-Will Messages :	·····································	

3、点击右侧的 Add New Topic Subscription, 订阅主题。

🥥 连接成功	Q 工单 消息 帮助文档 企业组织 财务 我
> 步骤1 Connection ● 运行中	
✓ 步骤2 Publish	✓ Subscriptions
Topic : O V Retain	Add New Topic Subscription
Message :	
publish 如果主题没有设置发布权限,会导致连接断开	
✓ 步骤3 Messages	

4、在弹出的 **Topic** 栏输入 device/up, Qos 默认 0 即可,点击"确定"即订阅这个主题。

	10.5k 13		
Topic	device/up	0	
	p.		

5、在 Message 下就可看到主机上报的数据。也可订阅主题 device/disconnect 查 看设备断开连接的信息,需设备配置物联网相关选项,详细操作说明见附录 2。

v 步骤2 Publish		✓ Subscriptions
opic :	? QoS: 0 ∨ Retain □	Add New Topic Subscription
Message :		Qos: 0 device/up
		Oos: 0
nublish 如果主要	1211年12月11日 - 今日改造法断开	device/disconnect
publish 如果主题 / 步骤3 Messages 2020/3/19 上午11:14:02	設有设置发布权限,会导致连接新开 Topic: device/up Qos: 0	device/disconnect
publish 如果主题 步骤3 Messages 2020/3/19 上午11:14:02 {"type":"up","time":"20: 18.024 1"]}	設有设置发布权限,会导致连接新开 Topic: device/up Qos: 0 200319111358*,*dev*:*GNC_NIO*,*aiolist*:[*1 0	device/disconnect

6、在 Publish 下的 Topic 栏输入控制命令的主题: device/control

可控制测试设备 GNC-NIO 的继电器 1^{~4} 闭合(D09[~]D012),下发的控制命令的 JSON 格式请参考设备说明。

步骤四. 通过 MQTT.fx 客户端连接测试

安装并打开 MQTT.fx 客户端,点击配置按钮。



点击"+",新建连接。以上述创建的 testsoft 用户为例,连接配置如下:

Profile Name: 自定义

Profile Type: MQTT Borker

Broker Address: yourendpoint.mqtt.iot.gz.baiduce.com

Boker Port: 1883

Clinet id: 自定义或随机生成

Username: yourendpoint/设备名称,见用户列表 **Password:** 为步骤一中,2.2.3 创建的 software **客户端身份密钥**

Edit Connection Profiles	
New Profile	
local mosquitto	Profile Name baidu-datatype-gnc-nio-test
	Profile Type MQTT Broker
	MQTT Broker Profile Settings
	Broker Address wnc8qgj.mqtt.iot.gz.baidubce.com
	Broker Port 1883
	Client ID f315223818fb4b0696e8850f20043db2 Generate
	General User Credentials SSL/TLS Proxy LWT
	User Name wnc8qgj/testsoft
	Password
de la composition de la compos	
All and the second s	Cancel OK Apply

Broker Address 和 Boker Port:

项目名称/Endpoint	类型	描述	地址
<mark>data_test</mark> wnc8qgj	数据型	2	tcp://wnc8qgj.mqtt.iot.gz.baidubce.com:1883 ssl://wnc8qgj.mqtt.iot.gz.baidubce.com:1884 wss://wnc8qgj.mqtt.iot.gz.baidubce.com:443
Username:			
用户名	描述		创建时间
wnc8qgj/testsoft	₫		2019-06-25 09:22:26

配置完成后,点击"Connect",即可成功连接。

Disconnect

在 Subscribe 界面中订阅主题: device/up,即可在该界面看到设备的上报数据。 也可订阅主题 device/disconnect 查看设备断开连接的信息。

baidu-deb			• 🔅 Connect	Disconnect				••
Publish Su	bscribe Scripts	Broker Status	Log					
device/up			Subscribe			Qo50 Qo51 Qo52	Autoscroll	0;*
device/disconnect		•	device/disconnect				Detained	1
	Dump Messages Mut	e Unsubscribe	device/up				Retained	2
device/up	Dump Messages Mut	e Unsubscribe					Retained	QoS 0
	and a second sec		device/up					QoS 0
Topics Collector (0)	Scan	Stop o ≋▼						
			device/up					3
			19-03-2020 11:18:44	.40724572				QoS 0
			{"type":"up", t	1me":"202003191	11840", dev : G	NC_NIO","alotist":["	1 0 12.592 1]	}

步骤五. SSL/TLS 连接

上述步骤一到四, 演示了网控物联网设备以 TCP 方式连接到百度天工数据型项目, 并通过百度天工物接入平台和 MQTT 客户端进行双向通信。对于安全级别要求较高 的场合, TCP 方式便不再适用, 此时需要通过 SSL/TLS 连接云平台, 以提高数据传 输安全性。创建策略和用户, 以及连接成功后进行在线调试等功能对于两种连接方 式均相同, 此处不多赘述。

网控设备的连接到百度天工数据型项目的物联网设置中,SSL/TLS 连接的配置类型 分为三种,对应三个不同的安全级别,由低到高分别为 CA 签名的服务器(不强制 证书检查),CA 签名的服务器(强制证书检查),自己签名的证书。

CA 签名的服务器用户身份:

以设备端为例, CA 签名的服务器(不强制证书检查)和 CA 签名的服务器(强制证书检查)两种连接方式的身份创建,与步骤一一致,即密码认证。

创建身份		
	1 创建身份 > 2 设置策略	> 3 配置确认
* 名称:	device	? 📀
* 认证方式	: 〇 证书认证 💿 密码认证 🛽	? 📀
		下一步取消

这里依然使用之前创建的用户"gnc_nio"来连接。

wnc8qgj/gnc_nio

1、CA 签名的服务器(不强制证书检查) **连接方式:** SSL **证书类型:** CA 签名的服务器 **端口号:** 1884

保存,重启即可。

 物联网设置 							
读配置 部分产品还需要在系统设置当中选择对应的数据上报方式或者协议							
中心MOTT服务器1设置 中心MOTT服务器2设置							
MQII协议版本 缺省 ▼ QOS O(almost once) ▼ 保持连接的时间间隔 120 秒 发布数据的超时	时间 15 秒						
■清除斷开期间服务器缓存的下发命令(Clean session) ■保持最后发布的内容(Retain),很多云不支持此选项							
□ 启用断开发布信息功能(Will),很多云不支持此选项							
町井信息的QUS U ▼ 【保持友布的助井信息(Will Retain) 町井信息的话题 devices/g	nc-n10/mes:						
连接方式 SSL ▼							
SSL/TLS连接设置	۲						
业书类型 CA登名的服务器(CA signed server certificate) ▼ □强制证书检查							
下传证书文件							
CA:1521字节 设备证书:1585字节 设备密钥:1676字节 证书格式:PEM							
物联网接入中心类型	-2						
服务器域名 wnc8qgj.mqtt.iot.gz.baidubce.com							
端口号 1884 (TCP缺省1883, SSL缺省1884)							
项目类型 数据型项目 ▼							
项目名 设备名(设备型-物影子名称,数据型-指定的用户名)							
wnc8qgj gnc_nio							
密码 uv							
数据型的上报话题(一般设device/up)数据型的控制话题(一般设device/control)							
device/up device/control							
以上的话题设置要与百度物接入当中的策略设置一致							

2、CA 签名的服务器(强制证书检查)

连接方式: SSL

证书类型: CA 签名的服务器

勾选强制证书检查。

下传证书文件: 百度天工根证书《root_cert.pem》

选择CA文件	
D:\BaiduDeviceCA\Bai	duRootCA\root_cert.pem
证书格式	
证书格式 ◎ PEM(文本)	● DER (二进制码)
证书格式 ◉ PEM(文本)	●DER(二进制码)

端口号: 1884

保存,重启即可(新下传的证书文件会覆盖旧文件)。

物联网设置	
读配置 部分产品还需要7	
中心MQTT服务器1设置 中心MQTT服务器2该	2置
☑ 启用	保存
MQTT协议版本 缺省 QOS O(almost onc.	e)
□ 清除断开期间服务器缓存的下发命令(Clean	session) 保持最后发布的内容(Retain),很多云不支持此选项
启用断开发布信息功能(Will),很多云不支持	此选项
断开信息的QOS 0 🔻 🗌 保持发布的断开	F信息(Will Retain) 断开信息的话题 devices/gnc-nio/mes:
连接方式 SSL ←	
SSL/TLS连接设置	
证书类型 CA签名的服务器(CA signed serve	☆r certificate) ▼
下传证书文件	
CA:1521字节 设备证书:1585字节 设备密	密钥: 1676字节 证书格式: PEM
物联网接入中心类型 百度天工	•
百度智能云	
服务器域名 wnc8qgj.mqtt.iot.gz.baidub	ice. com
端口号 1884 (TCP缺省1883,	SSL缺省1884)
项目类型 数据型项目 ▼	
项目名 设备	→名(设备型物影子名称,数据型-指定的用户名)
wnc8qgj gnc	_nio
密码 classification v	
数据型的上报话题(一般设device/up)	数据型的控制话题(一般设device/control)
device/up	device/control
以上的话题设置要与百度物接入当中的策略设置	是一致

自己签名的证书用户身份:

设备端的 SSL/TLS 连接的配置为自己签名的证书时,创建身份选择证书认证。

	1 创建身份 > (2) 设置策略 > (3) 配置确认
* 名称:	device_ssl	?
<u>*</u> 认证方式	: 💿 证书认证 🔿 密码认证 <table-cell> 🍳</table-cell>	

同样的选择设备端策略 device_policy, 然后在配置确认窗口"点击下载"证书及密钥。

创建身	11分	
	✓ 创建身份 > ✓ 设置策略 > 3 配置确认	
S	身份	
	名称: device_ssl	
	证书及密钥: 点击下载 请合理保管证书及密钥,密钥丢失无法找回,只能重新生成	
	策略	
	名称: device_policy	
	确议	L

会生成如图的证书文件,分别为设备证书、设备公钥、设备私钥和百度天工根证书。

📄 cert	-and-keys (2). txt☑ 不建议使用w	indows记事本打开	4
1	#The following is the client certificate.		^
2	BEGIN CERTIFICATE		
3	MIIEUzCCAzugAwIBAgIDAlnxMA0GCSqGSIb3DQEBCwUAMDMxFjAUBgNVBAMMDWlv	7+DEGINZUEND	
4	dC5iYWlkdS5jb20xDDAKBgNVBAsMA0JDRTELMAkGA1UEBhMCQ04wHhcNMjAwMzIw	—— XI BEGINEJEND	
5	MDM0MTE1WhcNNDAwMzE1MDM0MTE1WjBtMQ4wDAYDVQQKDAVCYWlkdTELMAkGA1UE	之间为一个面分	
6	BhMCQ04xQDA+BgNVBAMMN2RldmljZV9zc2wud25jOHFnai5mODM0NjAxNC0wZjVl		
7	LTQzNDYtODBmMS0xMmEzYWU2NTEwZGMxDDAKBgNVBAsMA0JDRTCCASIwDQYJKoZI		
8	hvcNAQEBBQADggEPADCCAQoCggEBAKAKT13QbfW0br3UEyOSAHfEJBm+v++XYa4K		
9	NTfmQRFqg6G+2q6dIhANkb6Hw0yFZTJdu8z5yJjAbwTyp0sW4sho3G+j/rRAudRr		
10	3x4a/VW1kV7RhT1wtN+9DbOQ2h8U0Hsc4ojvbLXiI+YXd1r7fyUR370hwAgZMhCc		
11	g1FczriMN5tX9EPLeB1Q9pfDP/SzUCggr1MyOFHeQJzpwxWuZe4Ohr5c4qIdmKPm		
12	reSlsbVMhMQq6c727YUAEisBUq5F8bG+obhcGYRPdmglXdwcIPp25Ahxhf4PivHG		
13	5qetgqBFxt+CWC1DmLJdL0Bf18LvJVmYKrHKgWsPy/N9RhqXF5sCAwEAAaOCATQw		
14	ggEwMB0GA1UdDgQWBBTltddpnRnNrhZQkvWVlN6SEGYQKjAMBgNVHRMBAf8EAjAA	设备证书	
15	MB8GA1UdIwQYMBaAFN0I5BWf1vz8AWv7jUq31dsFcI9jMG0GA1UdHwRmMGQwYqBg	*	
16	oF6GXGh0dHA6Ly9wa2lpb3YuYmFpZHViY2UuY29tL3YxL3BraS9jcmw/Y21kPWNy		
17	bCZmb3JtYXQ9UEVNJmlzc3Vlcj1DPUNOLENOPWlvdC5iYWlkdS5jb20sT1U9QkNF		
18	MEIGCCsGAQUFBwEBBDYwNDAyBggrBgEFBQcwAYYmaHR0cDovL3BraWlvdi5iYWlk		
19	dWJjZS5jb20vdjEvcGtpL29jc3AwDgYDVR0PAQH/BAQDAgP4MB0GA1UdJQQWMBQG		
20	CCsGAQUFBwMCBggrBgEFBQcDBDANBgkqhkiG9w0BAQsFAAOCAQEAUK7na7iHHaY1		
21	jm7tsluy17dgeCIBaOcgeC0AjrnZkEUSDqRQNMCq3addeSJiVt/crAb52mdsKfkz		
22	3nqs8eXNMB0hxIJgLz9G3OMQpYaF3sFYmt2BaZ8D/kW1612LgaxjZP1tbL88et50		
23	EMvy2QIvWx8w6DV7GgpFjRQUwTJJvGMJELluKGInrQUjLrcfY9CkS3uFjQRybcWN		
24	aMBzLAjm/uLIAKtMXX9NZa91Pdpmo6ULYXziJ4jTeA3gqC+lpyz4fgbPRRTMoTUD		
25	g0C2EFF1/fhMxvo64XQYi1bgyH1C7xEcGnxVixEmC9JZ50KOiM1bk1BZHhhLBSRN		
26	r4EwgxC1OA==		
27	END CERTIFICATE		
28		四女八相	
29	BEGIN PUBLIC KEY	以 宙公切	
30	MIIBIJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoApPXdBt9bRuvdQTI5IA	*	
31	d8QkGb6/75dhrgo1N+ZBEWqDob7arp0iEA2RvofDTIV1M127zPnImMBvBPKnSxbi		

设备的 SSL/TLS 配置要用到设备证书、设备私钥和百度天工根证书。

将 CERTIFICATE 这段复制到文本中另存为 clientcert.cer。

🔚 clientcert. cer 🛙]
---------------------	---

😑 clie	itcert. cer 🗹	۶.
1	BEGIN CERTIFICATE	
2	$\tt MIIEUzCCAzugAwIBAgIDAlnxMA0GCSqGSIb3DQEBCwUAMDMxFjAUBgNVBAMMDWlv$	
3	dC5iYWlkdS5jb20xDDAKBgNVBAsMA0JDRTELMAkGA1UEBhMCQ04wHhcNMjAwMzIw	
4	MDM0MTE1WhcNNDAwMzE1MDM0MTE1WjBtMQ4wDAYDVQQKDAVCYWlkdTELMAkGA1UE	
5	BhMCQ04xQDA+BgNVBAMMN2RldmljZV9zc2wud25jOHFnai5mODM0NjAxNC0wZjVl	
6	$\tt LTQzNDYtODBmMS0xMmEzYWU2NTEwZGMxDDAKBgNVBAsMA0JDRTCCASIwDQYJKoZI$	
7	hvcNAQEBBQADggEPADCCAQoCggEBAKAKT13QbfW0br3UEyOSAHfEJBm+v++XYa4K	
8	NTfmQRFqg6G+2q6dIhANkb6Hw0yFZTJdu8z5yJjAbwTyp0sW4sho3G+j/rRAudRr	
9	3x4a/VW1kV7RhT1wtN+9DbOQ2h8U0Hsc4ojvbLXiI+YXd1r7fyUR370hwAgZMhCc	
10	g1FczriMN5tX9EPLeB1Q9pfDP/SzUCggr1MyOFHeQJzpwxWuZe4Ohr5c4qIdmKPm	
11	reSlsbVMhMQq6c727YUAEisBUq5F8bG+obhcGYRPdmglXdwcIPp25Ahxhf4PivHG	
12	5qetgqBFxt+CWC1DmLJdL0Bf18LvJVmYKrHKgWsPy/N9RhqXF5sCAwEAAaOCATQw	
13	ggEwMB0GA1UdDgQWBBTltddpnRnNrhZQkvWVlN6SEGYQKjAMBgNVHRMBAf8EAjAA	
14	MB8GA1UdIwQYMBaAFN0I5BWf1vz8AWv7jUq31dsFcI9jMG0GA1UdHwRmMGQwYqBg	
15	oF6GXGh0dHA6Ly9wa2lpb3YuYmFpZHViY2UuY29tL3YxL3BraS9jcmw/Y21kPWNy	
16	bCZmb3JtYXQ9UEVNJmlzc3Vlcj1DPUNOLENOPWlvdC5iYWlkdS5jb20sT1U9QkNF	
17	MEIGCCsGAQUFBwEBBDYwNDAyBggrBgEFBQcwAYYmaHR0cDovL3BraWlvdi5iYWlk	
18	dWJjZS5jb20vdjEvcGtpL29jc3AwDgYDVR0PAQH/BAQDAgP4MB0GA1UdJQQWMBQG	
19	CCsGAQUFBwMCBggrBgEFBQcDBDANBgkqhkiG9w0BAQsFAAOCAQEAUK7na7iHHaYl	
20	jm7tsluy17dgeCIBaOcgeC0AjrnZkEUSDqRQNMCq3addeSJiVt/crAb52mdsKfkz	
21	3nqs8eXNMB0hxIJgLz9G30MQpYaF3sFYmt2BaZ8D/kW1612LgaxjZP1tbL88et50	
22	EMvy2QIvWx8w6DV7GgpFjRQUwTJJvGMJELluKGInrQUjLrcfY9CkS3uFjQRybcWN	
23	aMBzLAjm/uLIAKtMXX9NZa9lPdpmo6ULYXziJ4jTeA3gqC+lpyz4fgbPRRTMoTUD	
24	g0C2EFF1/fhMxvo64XQYi1bgyH1C7xEcGnxVixEmC9JZ50KOiM1bk1BZHhhLBSRN	
25	r4EwgxC1OA==	
26	END CERTIFICATE	

将 RSA PRIVATE KEY 这段复制到文本中另存为 prikey. key。

📄 prik	ey. key 🛛	4 F
1	BEGIN RSA PRIVATE KEY	
2	MIIEowIBAAKCAQEAoApPXdBt9bRuvdQTI5IAd8QkGb6/75dhrgo1N+ZBEWqDob7a	
3	rp0iEA2RvofDTIV1Ml27zPnImMBvBPKnSxbiyGjcb6P+tEC51GvfHhr9VbWRXtGF	
4	PXC0370Ns5DaHxTQexzii09steIj5hd3Wvt/JRHfvSHACBkyEJyDUVzOuIw3m1f0	
5	Q8t4HVD218M/9LNQKCCvUzI4Ud5AnOnDFa517g6Gvlzioh2Yo+at5KWxtUyExCrp	
6	zvbthQASKwFSrkXxsb6huFwZhE92aCVd3Bwg+nbkCHGF/g+K8cbmp62CoEXG34JY	
7	LUOYs10vQF/Xwu81WZgqscqBaw/L831GGpcXmwIDAQABAoIBAGg4DpMzRkg5Zdxs	
8	nMIPNArKShAR7f/ifxPNRfbPFRR4XpwYI2SOoz38+CoxUvcj71CrRb8n8n+24RVB	
9	x7vYfXqw/swc6aMMe3dff/6k6NDF2pL6sl/eY4tIHAIRlFmlPlbN6p/t+sc/Ks2N	
10	/oXbPWMwjpklv14Gulmi8skrPNtkPF08GFW3CvY7lDqV3/bzUYW4gye4MjAtvJtV	
11	c2tGJL8TbWjeKk21S7IS4OHNhTNudZMVFm4uMsLMp6TcCnH/81ptd2DkOQmRtHdz	
12	5v1B9CVgL7g9zx3bgFtBUrH/hJFWhVwatLTffZMvoT8Y85k+0m9MBinE1txy+8Ca	
13	ERJqbwECgYEA1UmN9GBb9sAAWUOKIWj8j+xAHtSV92Jpt+phbBTGh9kVnygBwA8Z	
14	bYnBOFW7ttHBwXWWwE9jjr8YtNCe8QHaJzA4H103ZpUz+TdOHNDyiMWvBylTJSOl	
15	vEEEwUB8EtstV3fPwjqhBLiObYVSMD6VejdgOmoYECAC3k8b8UvlFEECgYEAwBb6	
16	WWv5m8w/BkOecOxEvgtTbb0InxWIloLklC7VCEqY1MxtnXhr9+dM5iTuhVOL3E+h	
17	aNV7J61+ZuGmd7YfxWew/reUyR4L5JiryXbjYXsRa7Do5n/q6nJRH9pG+r9zTo3V	
18	x46g4kA+5n8dtsOF4PBMCVe4AVrsV/8QsM7dxNsCgYB3r5bhE1GH3aZUcPoKVYek	
19	m8Y/hrvA3pDEi9mvdNkTUlY3wZN52v9B4JN0sWds57f6f6ngsKwFZmbO0GLgi1GH	
20	vB9Bqr1z6zYHG2nR8c6nwYa+Vgo6RQ6z3Sh16WG2kxeWhb0oGQ5SP95sxuuf9v6a	
21	Xoi5Pt/R7KSva2UauqQKAQKBgFvU4FyNrSgZbevtubpcicSdH4Zv/8YmAkWKUAKz	
22	nO640vWwwZqtrlg2wOGpuEoPFeb+Prkijhz66Vn/+Jh0fh3eo5QyabP4ZFEl18KZ	
23	zryUnFByo/VGJCVu/2+N568KhfKBBjm/6xQfCLMjBC6SrNdLqd4xjGtBb4nmC7Gr	
24	RARPAoGBAM9JKR14aJUBt2XLGk0TcLiFPqo4WH1fDowQQkTPablv5Rx8ciYOOEZU	
25	Ni6zlI11SftoxxcKSYFxF9SBkOc1Dey/h+tHaGPQr9juzYUpaGu0UhBYXaiFa3nP	
26	G1gtYvfjT3kPUO9qnBPGuObAX1FoXvgqmcIt6e59XNM+vpMEI71e	
27	END RSA PRIVATE KEY	

开头下载的百度天工根证书《root_cert.pem》与这里复制文本另存得到的证书相同,可略过。

再创建一个身份设置为上述 device_ssl 的设备端用户 gnc_nio_ssl 用于设备配置。

创建用户		×
⊘ 创建月	用户 > < 设置身份 > < 设置策略 > 4 配置确认	
设备		
名称:	gnc_nio_ssl	
身份		
名称:	device_ssl	
策略		
名称:	device_policy	
	确认	

3、自己签名的证书

连接方式: SSL

证书类型:自己签名的证书

下传证书文件:设备证书《clientcert.cer》、设备私钥《prikey.key》和百度 天工根证书《root_cert.pem》

选择CA文件	百度天工根证书
D:\BaiduDeviceCA\BaiduRootCA\r	root_cert.pem
选择设备证书文件	_ 设备证书
D:\BaiduDeviceCA\dev_nio_ssl\d	clientcert.cer
选择设备私钥文件	设备私钥
D:\BaiduDeviceCA\dev_nio_ssl\p	prikey.key 🛄
证书格式	
◎ PEM (文本)	DER(二进制码)

端口号: 1884

设备名: 设置了证书认证身份的用户名

密码:此时双向证书作为密码,此处为空。

保存,重启即可(新下传的证书文件会覆盖旧文件)。

读配置	÷	防产品还得	需要在系统设	出当中选择对原	立的数据上	报方式或礼	皆协议		
中心MQTT服务	5器1设置 中心	MQTT服务	器2设置						
🛛 启用						保	存		
QTT协议版本	缺省 ▼ Q0	S 0(almost	once) 🔻	保持连接的时间	间隔 120	秒 发	布数据的超	时时间	15 利
■清除断开期) ■启用断开发7	可服务器缓存的⊺ 布信息功能(\¥ill	、 发命令(CI),很多云石	lean session 「支持此选项) 📃 保持最	后发布的内容	š(Retain)	,很多云不	支持此选项	Ð,
断开信息的G E接方式 SS		🗌 保持发布	的断开信息(Wi	ll Retain)	断开信	息的话题	devices/	/gnc-nio/	mes:
正书类型 〔	^{反血} 自己签名的证书()	Gelf signe	d certificat	es) 🔹					
下传证	书文件	用户私钥文	件密码						
下传证 CA:1521字节	书文件 设备证书:15	用户私钥文 85字节	件密码 设备密钥: 167	4字节	证书格式:I	EM			
下传证 CA:1521字节 勿联网接入中心	书文件 设备证书:15)类型 百度天	用户私钥文 85字节 T	件密码 设备密钥: 167	4字节	证书格式: F	PEM			
下传证 CA:1521字节 Ø联网接入中心 百度智能云	书文件 设备证书: 15 公类型 百度天	用户私钥文 85字节 工	件密码 设备密钥:167	4字节	证书格式: F	PEM			
下传证 CA:1521字节 列联网接入中心 百度智能云 服务器域名	书文件 设备证书:15 2类型 百度天 wnc8qgj.mqtt	用户私钥文 85字节 工 	件密码 设备密钥: 167 aidubce.com	4字节	证书格式: I ▼	?ЕМ			
下传证 CA:1521字节 9联网接入中心 百度智能云 服务器域名 端口号	 书文件 设备证书:15 >次型 百度天 wnc8qgj.mqt1 1884 	用户私钥文 85字节 工 iot.gz.b: (TCP缺省	件密码 设备密钥: 167 aidubce.com 1883, SSL缺省	14字节	证书格式: F	EM			
下传证 CA:1521字节 勿联网接入中心 百度智能云 服务器域名 端口号 项目类型	 书文件 设备证书: 15 3次型 百度天 wnc8qgj.mqt1 1884 数据型项目 	用户私钥文 85字节 工 iot.gz.ba (ICP缺省	件密码 设备密钥: 167 aidubce.com 1883, SSL缺省	11884)	证书格式: I 	'ЕМ 			
下传证 CA:1521字节 吻联网接入中心 百度智能云 服务器域名 端口号 项目类型 项目名	 书文件 设备证书:15 次型 百度天 wnc8qgj.mqt1 1884 数据型项目 	用户私钥文 85字节 工 iot.gz.b: (TCP缺省	件密码 设备密钥: 167 aidubce.com 1883, SSL缺省 设备名(设备)	4字节 11884) 型-物影子名称,\$	证书格式:I	YEM))))))))			
下传证 不供证 可度智能云 服务器域名 端口号 项目类型 项目名 wnc8qgj	 书文件 设备证书: 15 3次型 百度天 wnc8qgj.mqt1 1884 数据型项目 	用户私钥文 85字节 工 iot.gz.ba (TCP缺省 ▼	件密码 设备密钥: 167 aidubce.com 1883, SSL缺省 设备名(设备; gnc_nio_ss	14字节 11884) 型物影子名称,ؤ 1	证书格式: I ▼ 数据型-指定	YEM 的用户名)			
下传证	 书文件 设备证书:15 次型 百度天 wnc8qgj.mqt1 1884 数据型项目 	用户私钥文 85字节 工 iot.gz.b: (ICP缺省 、 (ICP缺省	件密码 设备密钥: 167 aidubce.com 1883, SSL缺省 设备名(设备; gnc_nio_ss 证时,不需	24字节 〕 〕1884〕 型-物影子名称,貧 1 要密码	证书格式: I ▼ 数据型-指定	YEM 的用户名)			
下传证 不传证 如联网接入中心 雪度智能云 服务器域名 端口号 项目类型 项目名 wnc8qgj 密码 数据型的上报	 书文件 设备证书:15)类型 百度天 wnc8qgj.mqtt 1884 数据型项目 使用双 酸话题(一般设dex 	用户私钥文 85字节 工 (TCP缺省 (TCP缺省 (向证书认 vice/up)	件密码 设备密钥: 167 aidubce.com 1883, SSL缺省 设备名(设备: gnc_nio_ss 证时,不需 数据型	4字节 11884) 型-物影子名称, 1 要密码 的控制话题(一般	证书格式: I 数据型-指定 设device/c	YEM 的用户名) ontrol)			

同理, MQTT 客户端也可以 SSL/TLS 方式连接到百度天工物联网平台进行测试。 CA 签名的服务器统一使用之前创建的 testsoft 用户。

wnc8qgj/testsoft

1、CA签名的服务器(不强制证书检查)

Edit Connection Profiles	
baidu-datatype-gnc-nio-test baidu_datatype_gnc_nio_ssl gnc-nio-shadow local mosquitto	Profile Name baidu-datatype-gnc-nio-test Profile Type MQTT Broker
	MQTT Broker Profile Settings Broker Address wnc8qgi.mqtt.iot.gz.baidubce.com Broker Port 1884 用户名,密码依然需要 Client ID f315223818/b4b0696e8850r20043db2 Generate
	General User Credentials SSL/TLS Proxy LWT Enable SSL/TLS ✓ Protocol TLSv1.2 ✓ • CA signed server certificate
	CA certificate file CA certificate keystore Self signed certificates Self signed certificates in keystores
Second Comments	Kevert Cancel OK Apply

2、CA 签名的服务器(强制证书检查)

and datatype Bit no test		
aidu_datatype_gnc_nio_ssl	Profile Name baidu-datatype-gnc-nio-test	
nc-nio-shadow	Profile Type MOTT Broker	™OT
ocal mosquitto	Home type Might bloker	Manager 1
	MQTT Broker Profile Settings	
	Broker Address wnc8qgj.mqtt.iot.gz.baidubce.com	
	Broker Port 1884	
	用户名,密码依然需要 Client ID f315223818fb4b0696e8850f20043db2	2 Generate
	General User Credentials SSL/TLS Proxy LWT Enable SSL/TLS V Protocol TLSv1.2	
	CA signed server certificate	
	CA certificate file	
	CA certificate file CA Certificate File D:\BaiduDeviceCA\BaiduRootCA\root	_cert.pem
	CA certificate file CA Certificate File D:\BaiduDeviceCA\BaiduRootCA\root CA certificate keystore	_cert.pem
	CA certificate file CA Certificate File D:\BaiduDeviceCA\BaiduRootCA\root CA certificate keystore Self signed certificates	_cert.pem
	CA certificate file CA Certificate File D:\BaiduDeviceCA\BaiduRootCA\root CA certificate keystore Self signed certificates Self signed certificates in keystores	cert.pem
	CA certificate file CA Certificate File D:\BaiduDeviceCA\BaiduRootCA\root CA certificate keystore Self signed certificates Self signed certificates in keystores	_cert.pem
	CA certificate file CA Certificate File D:\BaiduDeviceCA\BaiduRootCA\root CA certificate keystore Self signed certificates Self signed certificates in keystores	_cert.pem
	CA certificate file CA Certificate File D:\BaiduDeviceCA\BaiduRootCA\root CA certificate keystore Self signed certificates Self signed certificates in keystores	_cert.pem
	CA certificate file CA Certificate File D:\BaiduDeviceCA\BaiduRootCA\root CA certificate keystore Self signed certificates Self signed certificates in keystores	_cert.pem
	CA certificate file CA Certificate File D:\BaiduDeviceCA\BaiduRootCA\root CA certificate keystore Self signed certificates Self signed certificates in keystores	_cert.pem
	 CA certificate file CA certificate File D:\BaiduDeviceCA\BaiduRootCA\root CA certificate keystore Self signed certificates Self signed certificates in keystores 	_cert.pem

3、自己签名的服务器

创建一个证书认证的客户端身份 software_ssl。

<u>*</u> 名称:	● 创建身份 》(2)设置策略 》(software_ssi	3)配置确认
* 认证方式:	◉ 证书认证 🔿 密码认证 🛛 🔮	

绑定客户端策略 software_policy, 然后下载证书及密钥。

创建身份	×
◇ 创建身份 > ◇ 设置策略 > 3 配置确认	
身份	
名称: software_ssl	
证书及密钥: 点击下载 请合理保管证书及密钥,密钥丢失无法找回,只能重新生命	龙
策略	
名称: software_policy	确认

与设备端一样操作,得到 MQTT 客户端连接的设备证书、设备私钥和百度天工根证书。

XE/U/		
⊘ 创建用	⊐ > ◇ 设置身份 > ◇ 设置策略 >	4 配置确认
设备		
名称:	testsoft_ssl	
身份		
名称:	software_ssl	
策略		
名称:	software_policy	
		通过

再创建一个身份设置为上述 software_ssl 的客户端用户 testsoft_ssl。

MQTT 客户端的连接配置:

Edit Connection Profiles	
baidu-datatype-gnc-nio-test baidu_datatype_gnc_nio_ssl gnc-nio-shadow local mosquitto	Profile Name baidu_datatype_software_ssl Profile Type MQTT Broker
	MQTT Broker Profile Settings
User Name wnc8qg	/testsoft_ssl Broker Address wnc8qgi.mqtt.iot.gz.baidubce.com
Password	Broker Port 1884
	只需要用户名,密码为空 Client ID 048cc6ea30fa4973bca1cbf5013b568e Generate
	General User Credentials SSL/TLS Proxy LWT
	Enable SSL/TLS 🗸 Protocol TLSv1.2
	CA signed server certificate
	CA certificate file
	Self signed certificates
	CA File D:\BaiduDeviceCA\BaiduRootCA\root_cert.pem,
	Client Certificate File D:\BaiduDeviceCA\software_ssl\clientcert.cer
	Client Key File D:\BaiduDeviceCA\software_ssl\prikey.key
	Client Key Password
	PEM Formatted 🗸
	 Self signed certificates in keystores
+ -	Revert OK Apply

附录 1: GNC-NIO 物模型属性说明

每一条属性表示 GNC-NIO 的一个数据监测点,添加的属性名称和数据类型请严格参照物模,否则会导致设备上报数据/下发控制异常。以下给出主要属性和全部物模型快照。

GNC-NIO 模拟量输入 AI1[~]AI8 属性:

添加属性		:
* 属性名称:	AI1	必须为AI1 [~] AI8
* 显示名称:	模拟量输入1	可自定义
* 类型:	number 🗸	必须为number
默认值:	请输入默认值	

GNC-NIO 开关量输入 DI1[~]DI8 属性:

* 属性名称:	DI1	必须为DI1 [~] DI8
* 显示名称:	漏水开关	可自定义
* 类型:	number 🗸	必须为number
默认值:	请输入默认值	
单位:	请输入单位	

GNC-NIO 继<u>电器输出 DO9[~]DO12</u> 属性:

* 属性名称:	DO9	必须为D09 [~] D012
* 显示名称:	继电器输出1	可自定义
* 类型:	number 🗸	必须为number
默认值:	请输入默认值	
单 位:	请输入单位]

GNC-NIO 输入输出的告警:

		必须为下列之一:
* 属性名称:	Al1Warn	AI1Warn AI8Warn DI1Warn DI8Warn D09Warn D012Warn
* 显示名称:	模拟量输入1告警	可自定义
* 类型:	number	✓ 必须为number
默认值:	请输入默认值	
单位:	请输入单位	
单位:	请输入单位	

GNC-NI0 全部物模型:

属性名称	显示名称	类型	默认值	单位
AI1	AI1	number		
AI1Warn	AI1Warn	number		
AI2	AI2	number		
AI2Warn	A21Warn	number		
AI3	AI3	number		
AI3Warn	AI3Warn	number		
AI4	AI4	number		
AI4Warn	AI4Warn	number		
AI5	AI5	number		
AI5Warn	AI5Warn	number		
AI6	AI6	number		
AI6Warn	AI6Warn	number		
A17	AI7	number		
AI7Warn	AI7Warn	number		
AI8	AI8	number		
AI8Warn	AI8Warn	number		
DI1	DI1	number		
DI1Warn	DI1Warn	number		
DI2	DI2	number		
DI2Warn	DI2Warn	number		
DI3	DI3	number		
DI3Warn	DI3Warn	number		
DI4	DI4	number		
DI4Warn	DI4Warn	number		
D15	DI5	number		
DI5Warn	DI5Warn	number		
DI6	DI6	number		
DI6Warn	DI6Warn	number		
DI7	DI7	number		
DI7Warn	DI7Warn	number		
DI8	DI8	number		
DI8Warn	DI8Warn	number		
DO9	DO9	number		
DO9Warn	DO9Warn	number		
DO10	D010	number		
DO10Warn	DO10Warn	number		

附录 2: 数据型项目设备下线与遗嘱消息

百度天工数据型项目对于 MQTT 协议的一些特性支持较好,这里对网控设备物联网的 MQTT 协议部分的配置的使用作简要说明。MQTT 协议版本, QOS, 保持连接的时间间隔 (Keep Alive Time) 和发布数据的超时时间 (Timeout)略过。

中心MQTT服务器1设置 中心MQTT服务器2设置

☑ 启用		保存		
MQTT协议版本 缺省 ▼ QOS O(almost once) ▼ 保持连接的时间间	1篇 120 秒 🛛	发布数据的超时时间	15	秒
 □ 清除断开期间服务器缓存的下发命令(Clean session) □ 保持最后 □ 自用断开发布信息功能(\Vill),很多云不支持此选项 	发布的内容(Retair	ì),很多云不支持此选	项	
断开信息的QOS 0 ▼ 🦳 保持发布的断开信息(Will Retain)	断开信息的话题	device/disconne	ct	

1. Clean session

■清除断开期间服务器缓存的下发命令(Clean session)

未启用: MQTT 客户端发布的控制命令,物接入服务将该消息保留 24 小时,设备再次连接后控制命令立即生效。

启用: 设备断开连接期间, MQTT 客户端发布的控制命令则被服务器清除, 设备再次连接后控制命令不会生效。

baidu_dati				- 0		Disconnect					A
Publish Sul	bscribe <mark>Sc</mark> r	ipts	Broker Status	Log							
device/contr	ol				Publish		005.0	0051	Qo52	Retained	00v

2, Retain

📃 保持最后发布的内容(Retain),很多云不支持此选项

未启用:当有新的 MQTT 客户端订阅了主题 device/up 时,只能接收到设备向 该主题发布的实时数据,若设备断开连接,则 MQTT 客户端只能等待设备重新连接 发布数据。

启用:服务器会给设备断开连接之前,往主题 device/up 发布的最后一条数 据添加一个 Retain 标记,当有新的 MQTT 客户端订阅该主题时,会立即接收到带有 Retain 标记的数据。

baidu_datatype_software_ssl	- Connect Disconnect		
Publish Subscribe Scripts Bro	ker Status Log		
device/up	▼ Subscribe	QoS 0 QoS 1 QoS 2 Autoscroll	
device/up Dump Messages Mute Unsub	device/up device/up	Retained	1 QoS 0 2 QoS 0
	Retain数据 device/up 20-03-2020 17:20:40.62440000	实时上报数据 Retained	1 QoS 0
Topics Collector (0) Scan Stop of	<pre>{"type":"up","time":"201912041712 st":[,{"id":61,"val":0.000000,"wa id":63,"val":0.000000,"warn":0},;</pre>	!43","dev":"M3A","addr":2,"sptype":"aio arn":0},{"id":62,"val":0.000000,"warn": "id":64,"val":0.000000,"warn":0}]}	","li 0},{"

3、Will 功能

📃 启用断开发布信息功能(Will),很多云不支持此选项

断开信息的QOS 0 ▼ ■保持发布的断开信息(Will Retain) 断开信息的话题 device/disconnect 遗嘱功能与断开信息的话题(遗嘱主题)配合使用,须与策略设置的主题一致,即 device/disconnect。

启用 Will 功能:测试 MQTT 客户端首先订阅遗嘱主题,当设备断开连接后, 由服务器向遗嘱主题发送设备预定义的遗嘱消息,通知已订阅了遗嘱主题的客户 端,该设备已下线。(设备下线3倍的 Keep Alive Time 时间后,服务器发出遗嘱 消息,120秒时为6分钟)

启用 Will Retain: 服务器会将设备最后一次断开连接时的遗嘱消息标记 Retain, 当有新的 MQTT 客户端订阅遗嘱主题时,会立即收到设备最近一次下线的 遗嘱消息。

baidu_datatype_software_ssl	Connect Discon	nect	A 🔴
Publish Subscribe Scripts Broker	Status Log		
device/up	Subscribe	QoS 0 QoS 1 QoS 2 Autoscrol	0;•
device/disconnect	device/disconnect	Retain	1 ed QoS 0
	device/disconnec	~	4 QoS 0
	が 断开连接的retain信息	断开连接的信息	
	device/disconnect 23-03-2020 09:12:29.33149742		4 QoS 0
Topics Collector (0) Scan Stop OG*	{"type":"disconnect","dev":"	GNC_NIO"}	