注册并登陆亚马逊国际网站 aws. com 创建账户(需要信用卡) 或者注册并登陆亚马逊中国区域账户(注册中国区域账户,需中国境内营业执照等资 质)。 申请 AWS 中国区域账户: <u>https://www.amazonaws.cn/sign-up/</u> 登陆 AWS 管理控制台: <u>https://cnnorthwest1.console.amazonaws.cn/console/home?region=cnnorthwest1&ref =pe</u>

3594660 413643570

本文档旨在帮助用户如何将网控设备接入到 AWS 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、在 AWS IoT 控制台注册设备

登陆 AWS 管理控制台,在服务列表找到 AWS IoT 或者使用搜索,进入 AWS IoT 控制台。



1、创建安全策略

AWS IoT 策略是 JSON 文档,用于允许网控物联网设备和客户端连接到 AWS IoT 消息代理,发送和接收 MQTT 消息以及获取或更新设备的影子。 在 AWS IoT 控制台,选择"安全"->"策略",进行创建策略。 这里创建2个策略,分别为设备端策略(网控物联网设备接入AWS IoT)和客户端策略(mqtt客户端接入AWS IoT)。

① 创建设备策略

名称以 gnc_device 为例。在操作输入框中输入: iot*, 会显示如下:

创建策略	
创建策略以定义一组授权操作。您可以对一个或多个资源 (物品、主题、主题筛选条件) 授权操作。要了解有关 loT 策略的更多信息, 策略文档页面。 名称 gnc_device	请访问 AWS loT
添加声明 策略声明定义资源可以执行的操作类型。	高级模式
f#TF iot:* 容渡 ARN	
arn:aws-cn:iot:cn-northwest-1:470326574341:topic/replaceWithATopic 效果 允许 □ 拒绝	

记住资源 ARN 一栏中的字符串,例如我们这个例子里面是: aws-cn:iot:cn-northwest-1:470326574341,中、外接入点的差别主要在 ARN 上,在编辑策略时候需注意

这个就是当前 AWS 账户对应的唯一 ARN。用该 ARN 字符串替换我司提供的 《aws_gnc_device. json》文件中的所有<yourARN>标记,如图。

🔛 aws_	_gnc_devi	oe. json🛛	• •
1	₽{		^
2		Version": "2012-10-17",	
3	ė "	Statement": [
4	¢		
5		"Effect": "Allow",	
6	ф.	"Action": [
7		"iot:Connect"	
8	-		
9	卓	"Resource": [
10		"arn: <yourarn>:client/\${iot:Connection.Thing.ThingName}"</yourarn>	
11	-		
12	F	b ^a	
13	₽ .		
14		"Effect": "Allow",	
15	皁	"Action": [
16		"iot:GetThingShadow",	
17		"iot:UpdateThingShadow"	
18	F		
19	F	"Resource": [
20		"arn: <yourarn>:thing/\${iot:Connection.Thing.ThingName}"</yourarn>	
21	-		
22	L		
23	F		
24		"Effect": "Allow",	
25	日	"Action": [
26		"iot:Publish",	
27		"iot:Keceive"	
28	L		
29	F	"Kesource": [
30		"arn:< <u>yourAKN</u> >:topic/device/\${iot:Connection.Thing.ThingName}/*",	¥



在创建策略页面,点击"高级模式",先清除输入框,然后拷贝替换过的 json 文本,粘贴到输入框中,最后点击"创建"完成设备端策略的创建。

创建策略	
创建策略以定义一组授权操作。您可以对一个或多个资源 (物品、主题、主题筛选条件) 授权操作。要了解有关 IoT 策略的更多信息 策略文档页面。 名称 gnc_device	、请访问 AWS loT
<pre>添加声明 策略声明定义资源可以执行的操作类型。 file file file file file file file fil</pre>	基本模式
	创建

注意:不正确的配置好策略,会造成设备无法登陆,或者无法控制。

② 创建客户端策略

名称以 gnc_soft 为例。查看 AWS 账户的 ARN,以及编辑策略 json 文档的操作参考上一步。

用 ARN 字符串替换我司提供的《aws_gnc_soft.json》文件中的所有<yourARN>标记,然后完成创建。

创建策略	
创建策略以定义一组授权操作。您可以对一个或多个资源 (物品、主题、主题输选条件) 授权操作。要了解有关 loT 策略的更多信息 策略文档页面。 名称 gnc_soft	息,请访问 AWS loT
<pre>添加声明 策略声明定义资源可以执行的操作类型。</pre>	基本模式
	创建

2、创建物品

在 AWS IoT 控制台,选择"管理"->"物品",进行创建物品,这里以网控物联网 多功能输入输出模块 GNC-NIO 为例。

① 选择"创建单个物品"。

创建 AWS IoT 物品	
loT 物品是云中的物理设备的表示形式和记录。任何物理设备都需要有物品记录才能使用 AWS loT。了解详情。	
注册单个 AWS IoT 物品 在注册表中创建物品	创建单个物品
批量注册多个 AWS IoT 物品 在注册表中为大量已经在使用 AWS IoT 的设备创建物品,或者注册设备以让它们准备好连接到 AWS IoT。	的建多个物品
取消	创建单个物品

②输入名称。物品类型,物品组和设置可搜索的物品属性请根据业务部署情况选择,此处略去。点击"下一步"。

翻翻 将设备添加到物品注册表	第1步供3 步
此步骤将在物品注册表中为您的设备创建注册表项和物品影子。 名称	
gnc-nio	
将类型应用于此物品 使用物品类型可通过为具有相同类型的物品提供一致的注册表数据来简化设备管理。类型可为物品提供一组常风属性和一个论	
的身份和功能。 物品类型	
未选择类型	

③选择"一键式创建证书"。

^{國議論區} 添加物品的证书	第2步(共3 步)
证书用于验证您的设备与 AWS IoT 的连接。	
一键式创建证书(建议) 这将使用 AWS IoT 的证书颁发机构生成证书、公有密钥和私有密钥。	會加加正书
利用 CSR 创建 基于您拥有的私有密钥上传您自己的证书签名请求 (CSR)。	土 利用 CSR 创建
使用我的证书 注册您的 CA 证书,并对一个或多个设备使用您自己的证书。	ĹΊλ
跳过证书并创建物品 稍后您需要向物品添加证书,您的设备才能连接到 AWS loT。	创建没有证书的物品

④选择**下载该物品的证书,私有密钥**和 AWS IoT 的根 CA (无需下载公有密钥),将其中的每一项都保存到您的计算机上,然后点击"激活"证书,最后选择"附加策略"。

特别注意: 私钥文件只能在这个页面下载, 如果过了这个页面就无法

再下载密钥文件,只能删除设备重建。

证书已创建!
下载这些文件并将其保存在安全的位置。证书是可以随时检索的,但在关闭此页面后就无法检索私有密钥和公有密钥。 要连接设备,您需要下载以下内容:
该物品的证书 8b8a2e3613.cert.pem 下载
公有密钥 8b8a2e3613.public.key 下载
私有密钥 8b8a2e3613.private.key 下载 1、下载证书
您还需要下载 AWS IoT 的根 CA: 2、激活证书
2015 3、附加策略
取消 完成 附加策略

根证书只需下载一次,所有设备使用同一个根证书。

用于服务器身份验证的 CA 证书

根据您使用的数据终端节点的类型以及您协商的密码套件, AWS IoT 服务器身份验证证书由以下根CA 证书之一进行签名:

VeriSign 终端节点 (传统)

• RSA 2048 位密钥: VeriSign Class 3 Public Primary G5 根 CA 证书 🖸

Amazon Trust Services 终端节点 (首选)

- RSA 4096 位密钥: Amazon Root CA 2。留待将来使用。
- ECC 256 位密钥: Amazon Root CA 3 2。
- ECC 384 位密钥: Amazon Root CA 4。留待将来使用。

这些证书都由 Starfield 根 CA 证书 记进行交叉签名。从 2018 年 5 月 9 日 AWS IoT Core 的推出开始,亚太 (孟买) 区域中的所有新 AWS IoT Core 区域都将仅处理 ATS 证书。

⑤在添加物品的策略页面,勾选之前创建的 gnc_device 策略,选择"注册物品"即可完成物品的创建。

上述创建的物品 gnc-nio 及其证书和密钥用于网控物联网设备接入 AWS IoT。

查看
查看
注册物品

⑥然后用同样的方法创建名为 ClientSoft 的物品,用于客户端接入 AWS IoT, 区别在于最后一步添加物品的策略时,勾选之前创建的 gnc_soft 策略,并下载 保存证书和密钥。

^{國鐵物品} 添加物品的策略	第3步供3 岁)
选择策略以附加到此证书:	
Q 搜索策略	
gnc_soft	查看
<pre>gnc_device</pre>	查看
1 个策略已选定	注册物品

补充:

在 AWS IoT 控制台,选择"安全"->"证书",进行证书的管理。 若物品绑定的证书未激活,显示"非活动"状态,如图。会导致设备或 MQTT 客 户端连接 AWS IoT 失败,可点击证书名称跳转到证书详情页。

🖗 AWS IOT	证书			创建
拉	搜索证书	Q		* •
门培训				
理	c583c3854b6514e20 ● ● 活动	1f9d4db853e61a539 🗩 ● 活动	0968590d917e62621 ● 活动	
全				
证书	•	•	•	
策略 CA	87eb786a32441e2db● ● 活动	e22acccc1470fb7c136.9. ● 活动	beee2b8f207345b5f0. ● 活动	
角色别名				
授权方	•	•	•	
动	Oacdc30f3167f9c2f29.★● 活动	4e06cb96cf08cd9f9c0● 活动	f0ac49b741d83f4183. 🖲 ● 活动	
试			L	
	•	•	•	
	8b8a2e36139855b72● ● 活动	c4148eda0688f7cf6fc. # ● 非活动		
	•	•		

选择"操作"->"激活"即可激活证书。还可以下载证书、查看对应的物品和 附加的策略。

		15
		激活
细信息	ARN 证书	以()月渡()古
略		11(11)
с л н	证书 Amazon 资源名称 (ARN) 用于唯一标识此证书。 了解详情	接受性胸
品		拒绝传输
	arn:aws-cn:iot:cn-northwest-1:470326574341:cert/c4148eda0688f7cf6fc	bd 撤销传输
		开始传输
		附加策略
	详细信息	附加物品
		下载
	发布者	删除
	OU=Amazon Web Services O\=Amazon.com Inc. L\=Seattle S1\=Washington C\=US 主题	
	CN=AWS IoT Certificate	
	创建日期	
	2020年3月6日 上午11:27:55 +0800	
	生双日期 2020年7月6日 上午11:25:55 ±0800	
	2020年3月8日 工十11.23.35 +0800 到期日期	

上述的 AWS IoT 的业务逻辑示意图如下。其中物品,证书和策略的可各自单独 创建,不分先后,只是需在创建后按照这种逻辑将三者关联起来。

物联网设备 <> gnc-nio	gnc_device
MQTTClient ClientSoft	gnc_soft

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,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。

连接方式: SSL

证书类型: 自己签名的证书

下传证书文件: 下传 AWS IoT 创建的物品 gnc-nio 对应的证书、密钥和根证书, 如图:

选择下传证书文件			<u>. </u>		>
选择CA文件		AWS IoT相	夏证书		
D:\aws certs\AmazonRoot	CA1.crt				•
选择设备证书文件		gnc-nio的	的物品	证书	
D:\aws certs\gnc-nio\8b	8a2e3613-	certificate	.pem.c	r	•
选择设备私钥文件		gnc-nio的	的私钥		
D:\aws certs\gnc-nio\8b	8a2e3613-;	private.pem	. key		•
证书格式					

物联网接入中心类型:亚马逊 AWS。下方的参数设置框自动切换到亚马逊 AWS-IOT 界面。

终端节点域名: gnc-nio 物品详情的"交互"页面,见下图:

物品		
gnc-nio ૠ型		操作
详细信息	该物品似乎已连接。	连接设备
安全性		
物品组	HTTPS	
账单组	使用此 Rest API 终端节点更新您的物品影子。了解详情 终端节点域名/Broker	: Address
影子	a50hc02lum220_ats int cn_nonthwest_1 amazonaws com cn	
交互	asydewziumssy-acs.idt.ch-norchwest-i.amazonaws.com.ch	

端口号:缺省为8883 **物品名称**:创建的设备端物品名称:gnc-nio 勾选**上报和处理影子数据。** 之后"保存","重启"设备。至此,设备的物联网配置完成。

	_3		×
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			
☑启用 保存			
MQIT协议版本 缺省 V QOS O(almost once) V 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: □启用断开发布信息功能(Will),很多云不支持此选项	持此选 ^I	顷	
断开信息的QOS 0 V 🗌 保持发布的断开信息(Will Retain) 断开信息的话题 device/dis	connec	st	
连接方式 SSL ~			
SSL/TLS连接设置			
W中央型 日口受有的W中(Self signed certificates) ↓			
下传证书文件 用户私钥文件密码			
CA:1206字节 设备证书:1220字节 设备密钥:1679字节 证书格式:PEM			
物联网接入中心类型 亚马逊A₩S ~			
亚马逊AWS-IOT			
AWS的连接方式必须是SSL或者Websock SSL,才能连接成功。而且必须是3个证书和密钥文件齐全			
终端节点域名 a59bc021um339-ats.iot.cn-northwest-1.amazonaws.com.			
端口号 8883 (缺省8883)			
物品名称 gnc-nio			
☑ 上报和处理影子数据			

三、通过影子查看设备状态

进入物品详情页面,选择"影子",查看物品影子文档。 动作接入到 DI1[~]DI8 的测试开关状态或改变接入到 AI1[~]AI8 的模拟量输入的大 小,可查看到设备的影子状态随之更新。

物品 > gnc-nio		
物品 gnc-nio 无类型		操作 -
详细信息	影子 ARN	
安全性		
物品组	影子 ARN 用于唯一标识此物品的影子。了解详情	
账单组	arn:aws-cn:iot:cn-northwest-1:470326574341:thing/gnc-nio	
影子		
交互	影子文档	MIRA 45+9
活动		加到政大,均同年時
任务	上次更新: 2020年3月6日下十1:18:56 +0800	
	<pre>{ "reported": { "D11": 0, "D1Warn": 0, "D12": 1, "D12Warn": 2, "D13Warn": 2, "D13Warn": 2, "D14": 1, "D14Warn": 2, "D15": 1, "D15Warn": 1, "D15Warn": 1, "D16": 1, "D16":</pre>	

点击"编辑",在编辑框中输入 "desired":{"D09":1},或 "desired":{"D09":0}, 如图,然后"保存"即可控制 NIO 的继电器 1-4(D09[~]D012)的状态,同时更新 影子状态。

影子文档

删除 取消 保存

上次更新: 2020年3月6日 下午1:23:40 +0800

影子状态:				
1 -	{·····································			
2	"desired":{"D09": 0},			
3 ~ 4	"reported": { "DI1": 0, "DI1Hape": 0			
5 6 7 8	"DI2": 1, "DI2Warn": 2,			

四、使用 AWS IoT 控制台在线测试

在 AWS IoT 控制台,选择"测试",进入在线 MQTT 客户端,在订阅主题输入框 输入: device/gnc-nio/up,点击"订阅主题"即可查看设备上报数据。

主题中第二级 gnc-nio 为物品名,您也可以使用通配符,例如: device/+/up 用来批量接收所有物品的上报数据。

AWS IOT	MQTT 客户端 ⑦	已以 iotconsole-1585556420738-2 的名义建立连接 🔻
监控	订阅	
入门培训	订阅主题	
管理	发去谐自夺一众主题	订阅 设备会在主题下发布 MQTT 消息。您可以使用此客户端订阅一个主题并接收
安全	《市内发生 十二級	这些消息。
行动		订阅主题
测试		device/gnc-nio/up
		最大消息捕获 ⑦
		100

在物品详情->交互页面查看与设备影子相关的主题。例如: 更新此物品影子文档的主题: **\$aws/things/gnc-nio/shadow/update/documents**

订阅	device/gnc-nio/up	导出清除。暂停
订阅主题 发布消息至一个主题	发布 指定要发布的主题和消息,QoS 为 0。	
device/gnc-nio/up 🗙	device/gnc-nio/up	发布到
device/+/up 🗙	1 { 2 "message": "Hello from AWS IoT console"	
\$aws/things/gnc-nio/shadow 🗙	3 }	
订阅列表,点击主题查看消息		
	device/gnc-nio/up 2020年3月30日下午4:46:12 +0	800 导出 隐藏
	{ "type": "up", "time": "20200330164610", "dev": "GNC_NIO", "aiolist": [上报数据
	"1 0 15.356 1"] }	