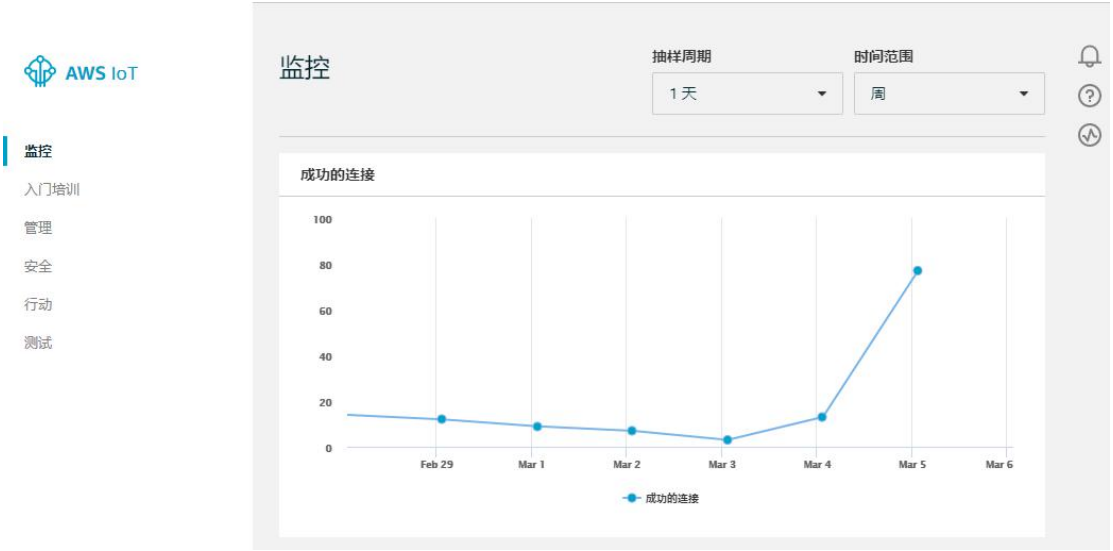
注册并登陆亚马逊国际网站 aws.com 创建账户（需要信用卡）
或者注册并登陆亚马逊中国区域账户（注册中国区域账户，需中国境内营业执照等资质）。
申请 AWS 中国区域账户：https://www.amazonaws.cn/sign-up/
登陆 AWS 管理控制台：
https://cnnorthwest1.console.amazonaws.cn/console/home?region=cnnorthwest1&ref_=pe_3594660_413643570

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。

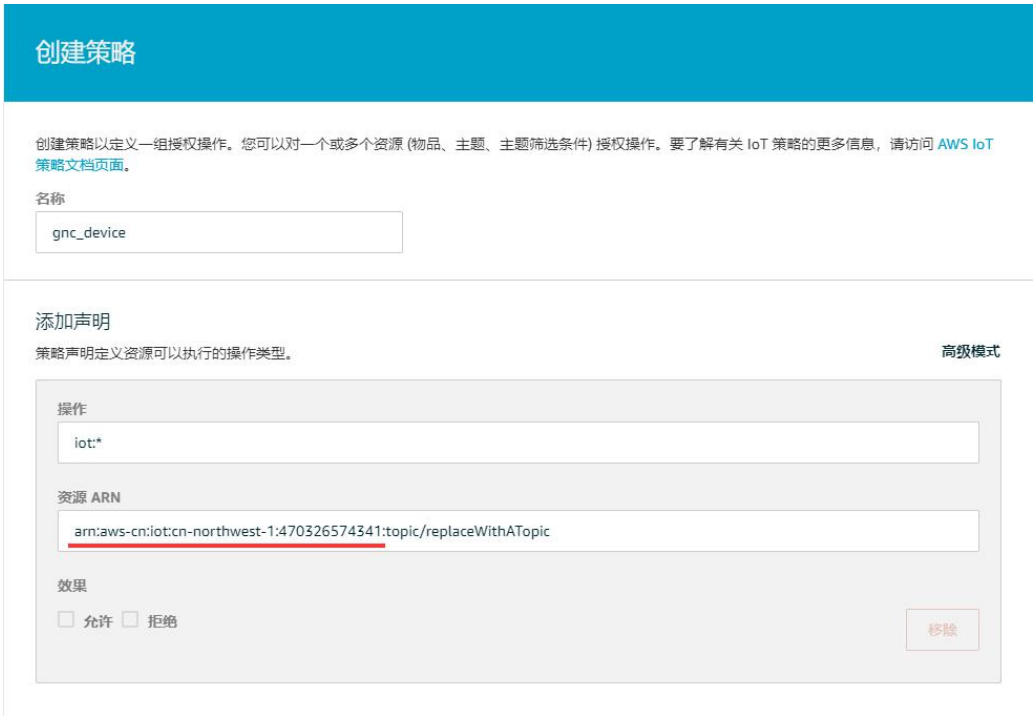


1、创建安全策略

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：



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。

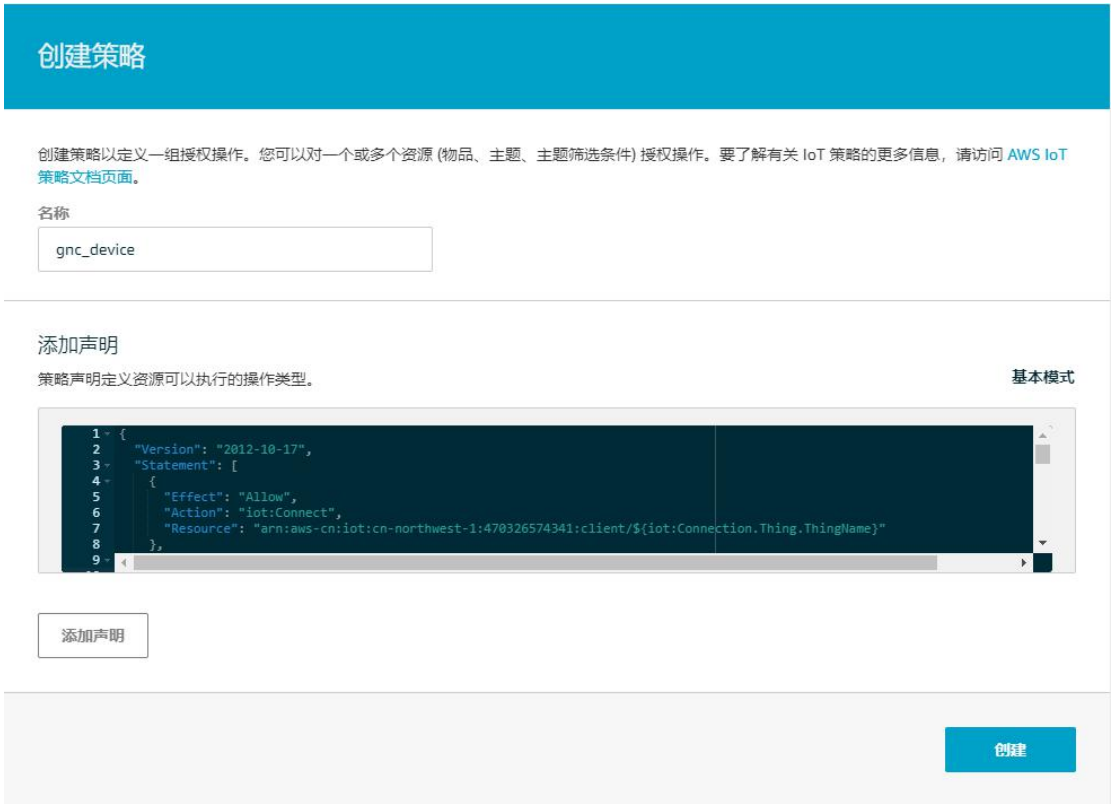
aws_gnc_device.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Connect"
      ],
      "Resource": [
        "arn:<yourARN>:client/${iot:Connection.Thing.ThingName}"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ],
      "Resource": [
        "arn:<yourARN>:thing/${iot:Connection.Thing.ThingName}"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish",
        "iot:Receive"
      ],
      "Resource": [
        "arn:<yourARN>:topic/device/${iot:Connection.Thing.ThingName}/*",
```

aws_gnc_device.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Connect"
      ],
      "Resource": [
        "arn:aws-cn:iot:cn-northwest-1:470326574341:client/${iot:Connection.Thing.ThingName}"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ],
      "Resource": [
        "arn:aws-cn:iot:cn-northwest-1:470326574341:thing/${iot:Connection.Thing.ThingName}"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish",
        "iot:Receive"
      ],
      "Resource": [
        "arn:aws-cn:iot:cn-northwest-1:470326574341: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。

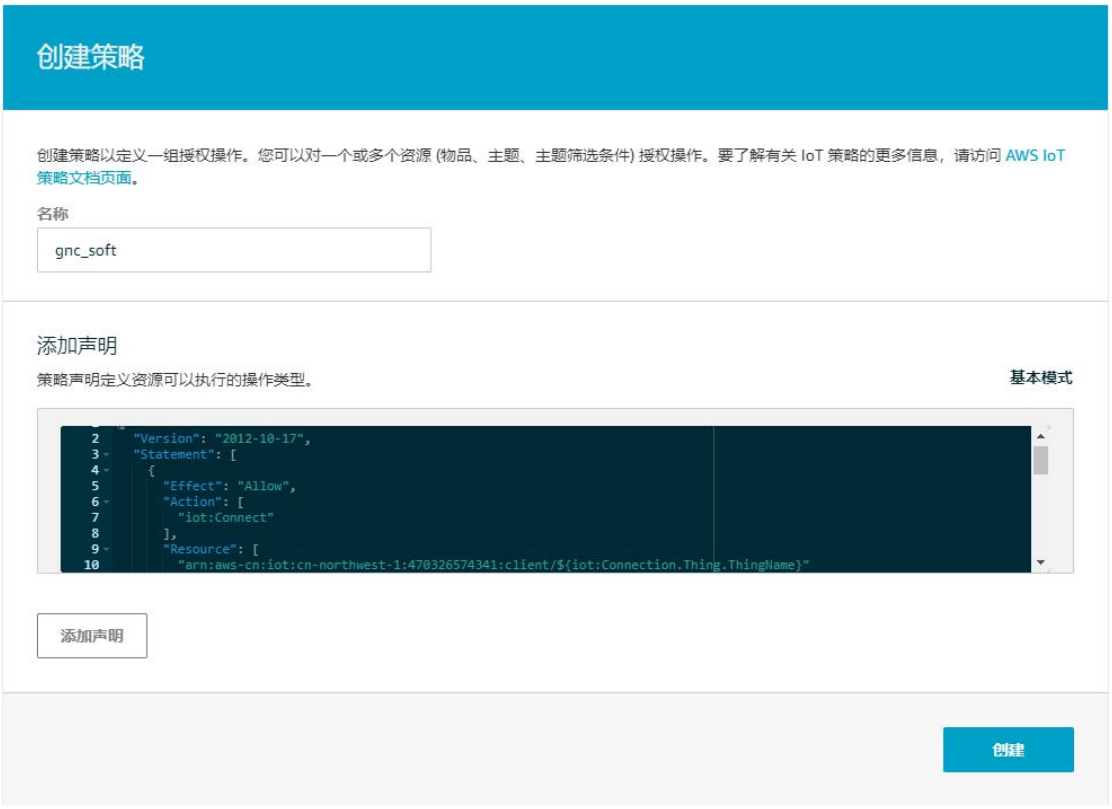


注意：不正确的配置好策略，会造成设备无法登陆，或者无法控制。

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。

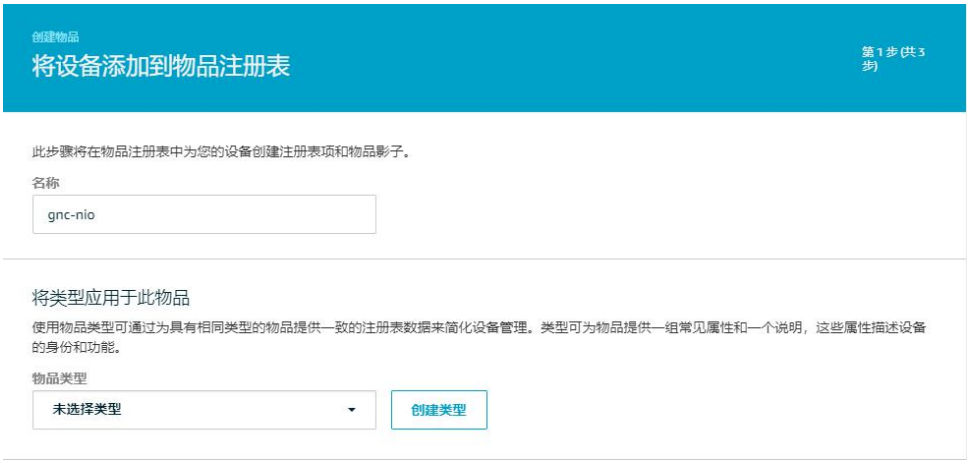


2、创建物品

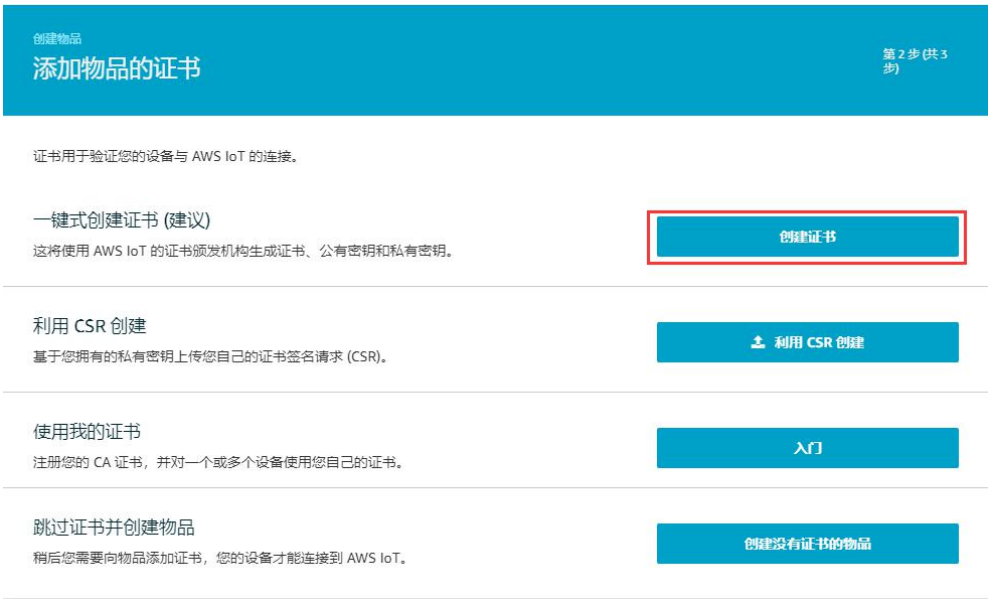
在 AWS IoT 控制台，选择"管理"->"物品"，进行创建物品，这里以网控物联网多功能输入输出模块 GNC-NIO 为例。

① 选择“创建单个物品”。

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”。



③选择“一键式创建证书”。



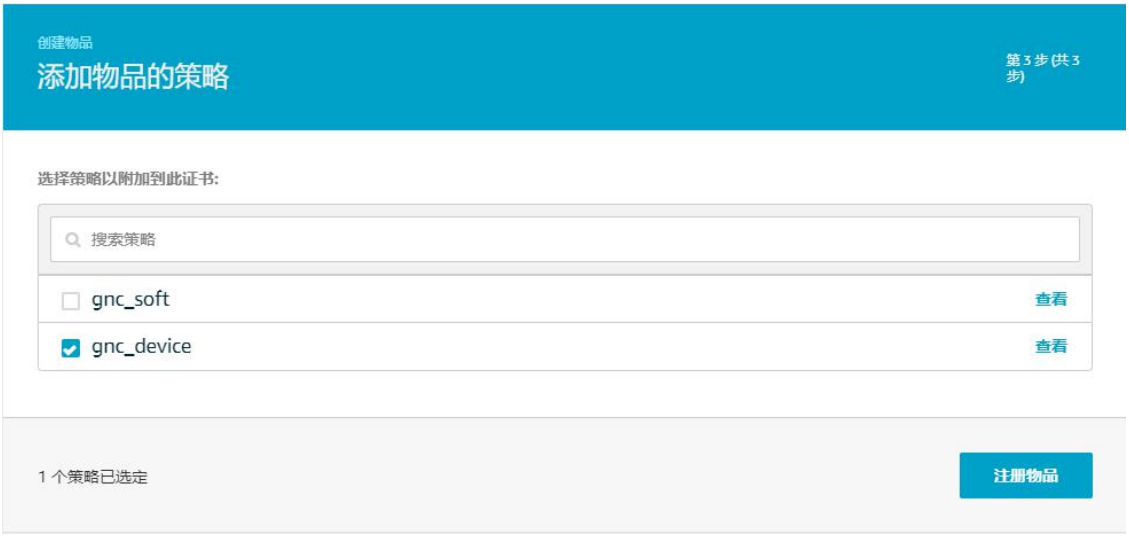
④选择**下载该物品的证书，私有密钥**和 **AWS IoT 的根 CA**（无需下载公有密钥），将其中的每一项都保存到您的计算机上，然后点击“激活”证书，最后选择“附加策略”。

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。

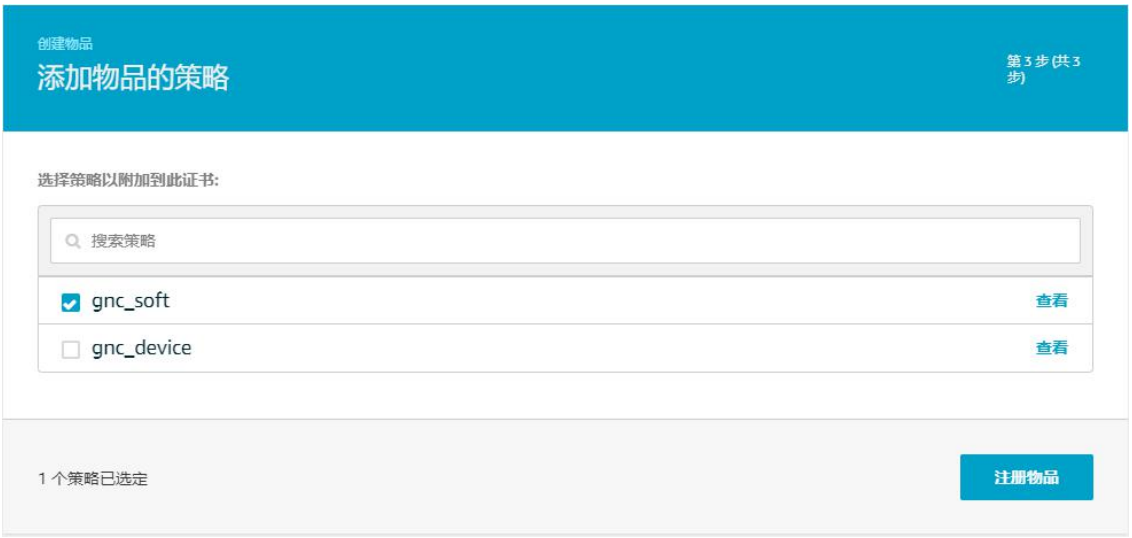
根证书只需下载一次，所有设备使用同一个根证书。

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。

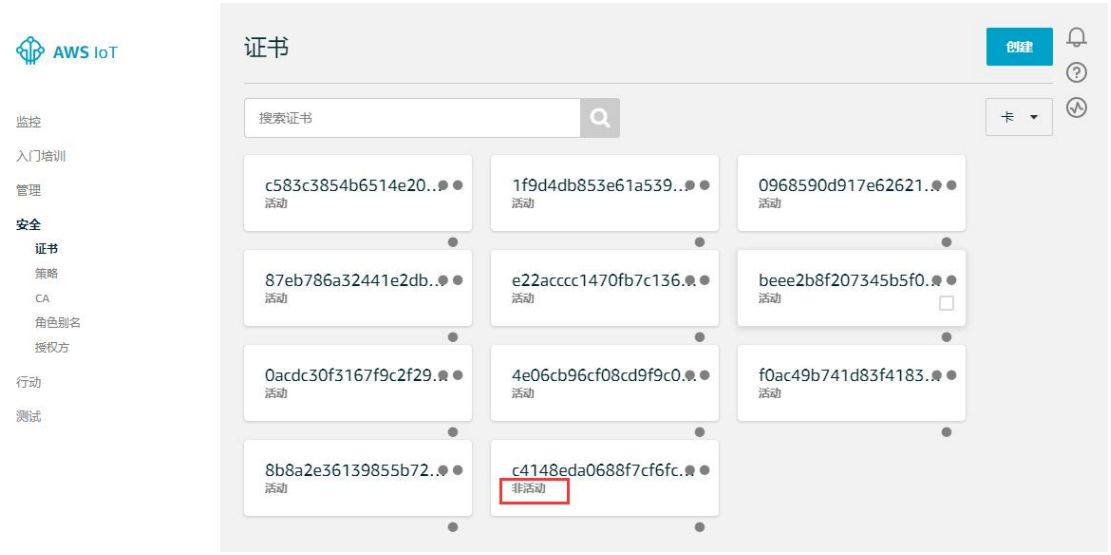
上述创建的物品 gnc-nio 及其证书和密钥用于网控物联网设备接入 AWS IoT。



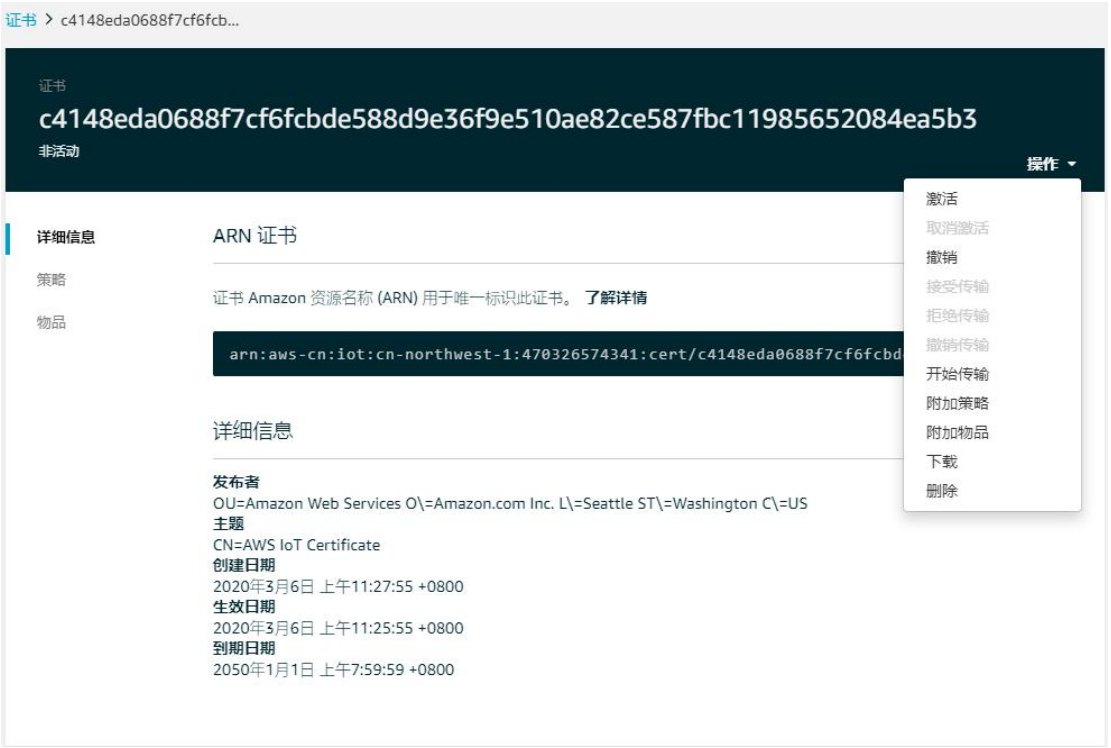
⑥然后用同样的方法创建名为 ClientSoft 的物品，用于客户端接入 AWS IoT，区别在于最后一步添加物品的策略时，勾选之前创建的 gnc_soft 策略，并下载保存证书和密钥。



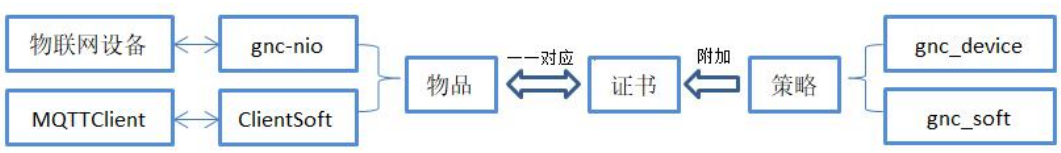
补充：
在 AWS IoT 控制台，选择"安全"->"证书"，进行证书的管理。
若物品绑定的证书未激活，显示“非活动”状态，如图。会导致设备或 MQTT 客户端连接 AWS IoT 失败，可点击证书名称跳转到证书详情页。



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。



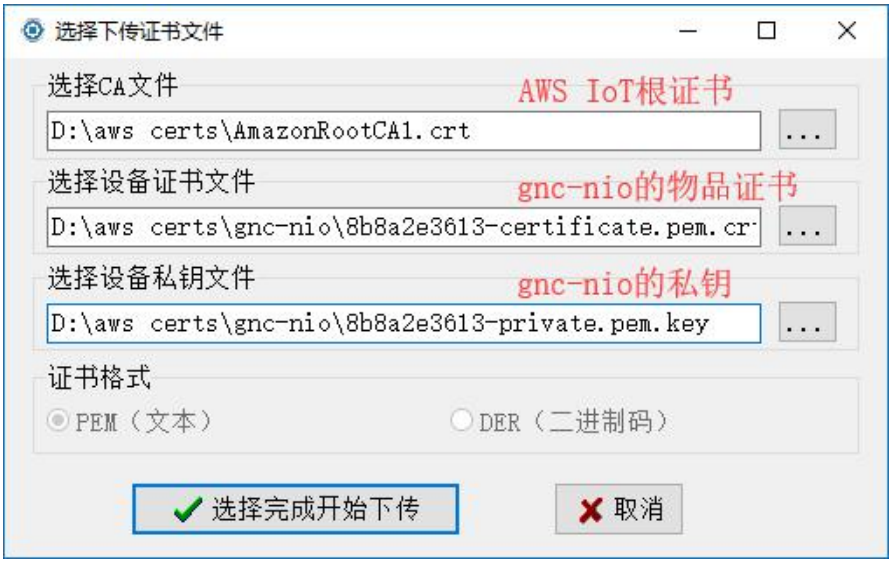
上述的 AWS IoT 的业务逻辑示意图如下。其中物品，证书和策略的可各自单独创建，不分先后，只是需在创建后按照这种逻辑将三者关联起来。



二、 网控物联网设备配置

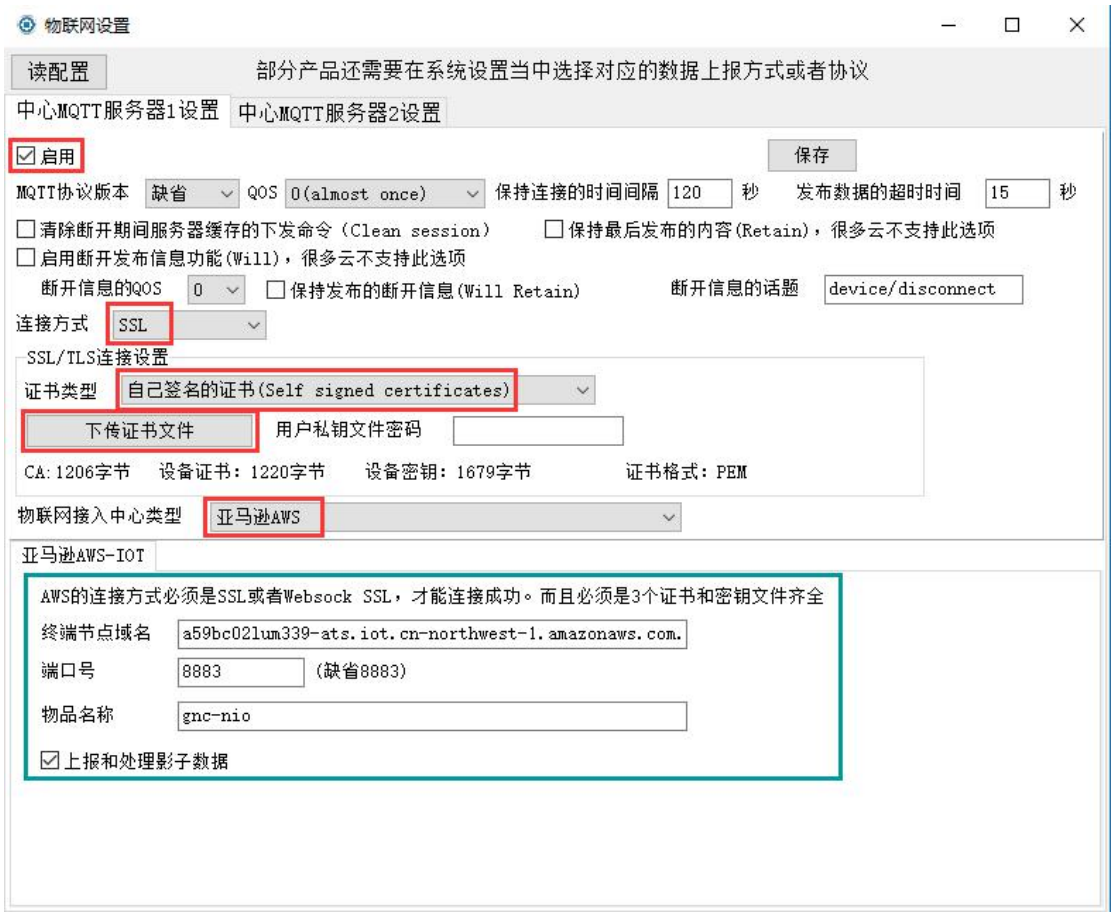
打开 GNC 设备发现与管理工具，发现认证登陆设备后，点击进入设备物联网配置界面。

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：



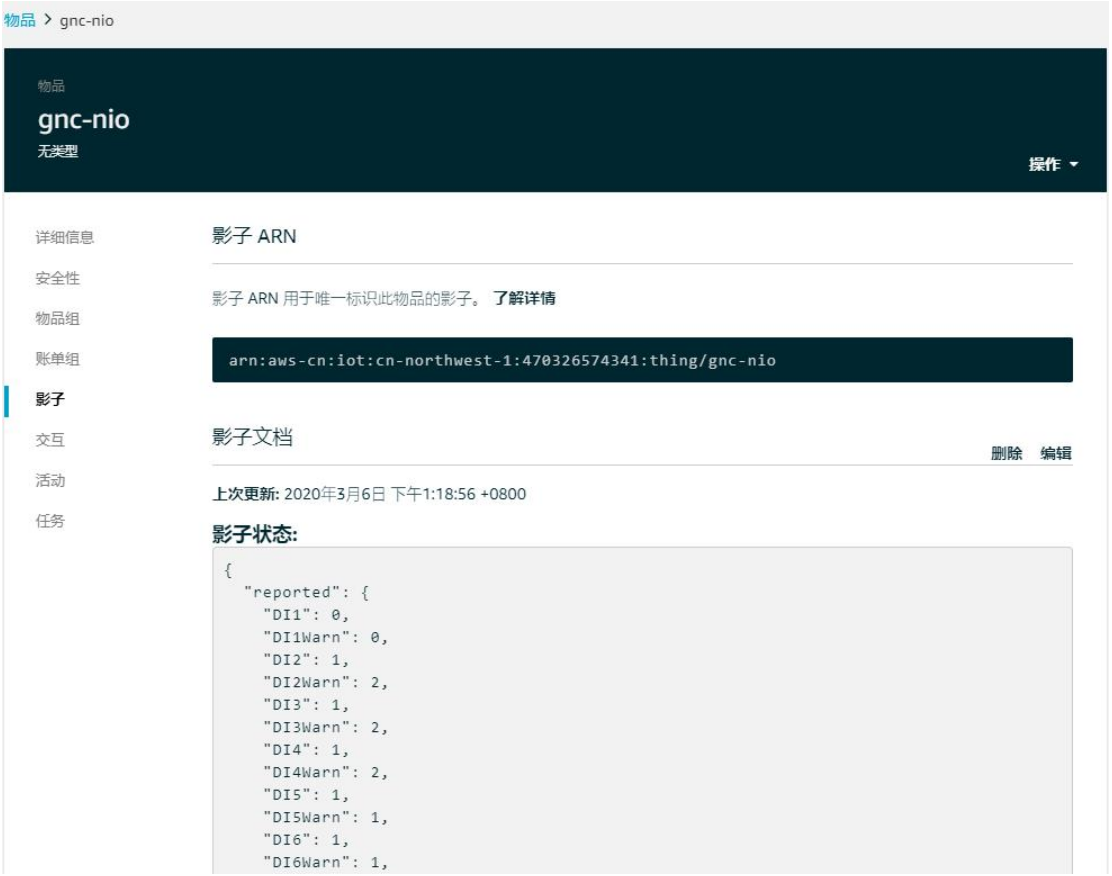
物联网接入中心类型：亚马逊 AWS。下方的参数设置框自动切换到亚马逊 AWS-IOT 界面。
终端节点域名：gnc-nio 物品详情的“交互”页面，见下图：

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。

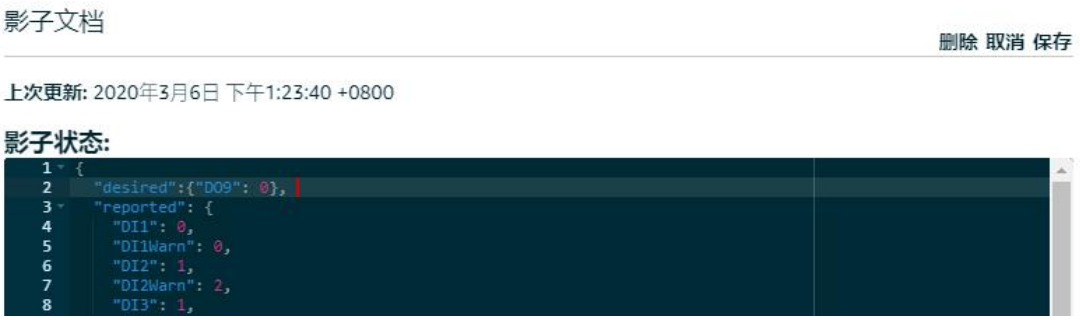

物联网设置
读配置
部分产品还需要在系统设置当中选择对应的数据上报方式或者协议
中心MQTT服务器1设置
中心MQTT服务器2设置
启用
保存
MQTT协议版本
缺省
QOS
0(almost once)
保持连接的时间间隔
120
秒
发布数据的超时时间
15
秒
清除断开期间服务器缓存的下发命令（Clean session）
保持最后发布的内容(Retain)，很多云不支持此选项
启用断开发布信息功能(Will)，很多云不支持此选项
断开信息的QOS
0
保持发布的断开信息(Will Retain)
断开信息的话题
device/disconnect
连接方式
SSL
SSL/TLS连接设置
证书类型
自己签名的证书(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AWS
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
a59bc02lum339-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。



点击“编辑”，在编辑框中输入
"desired":{"DO9": 1}, 或 "desired":{"DO9": 0},
如图，然后“保存”即可控制 NIO 的继电器 1-4(DO9~DO12)的状态，同时更新影子状态。



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。

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