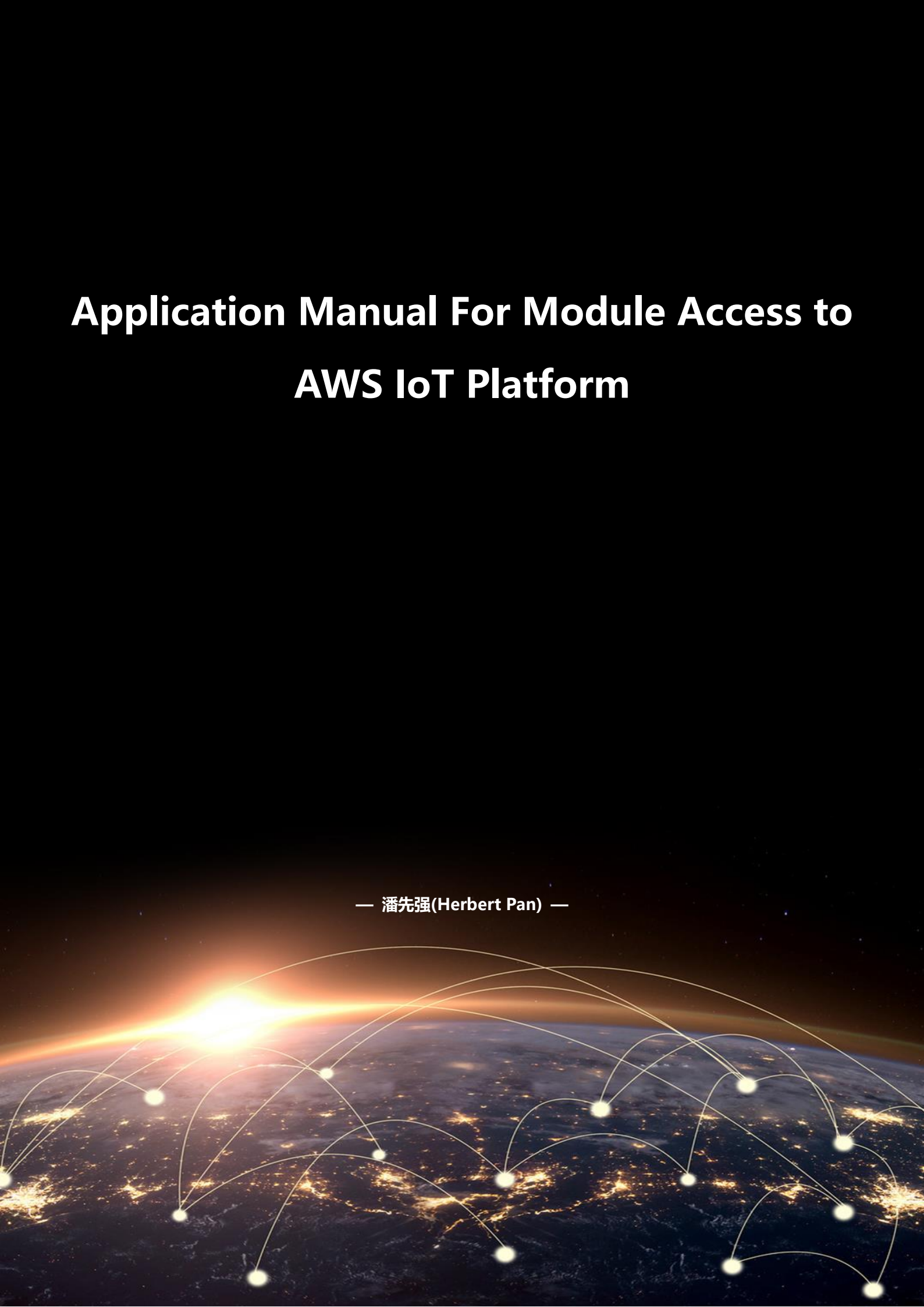
Application Manual For Module Access to AWS IoT Platform

— 潘先强(Herbert Pan) —



CONTENTS

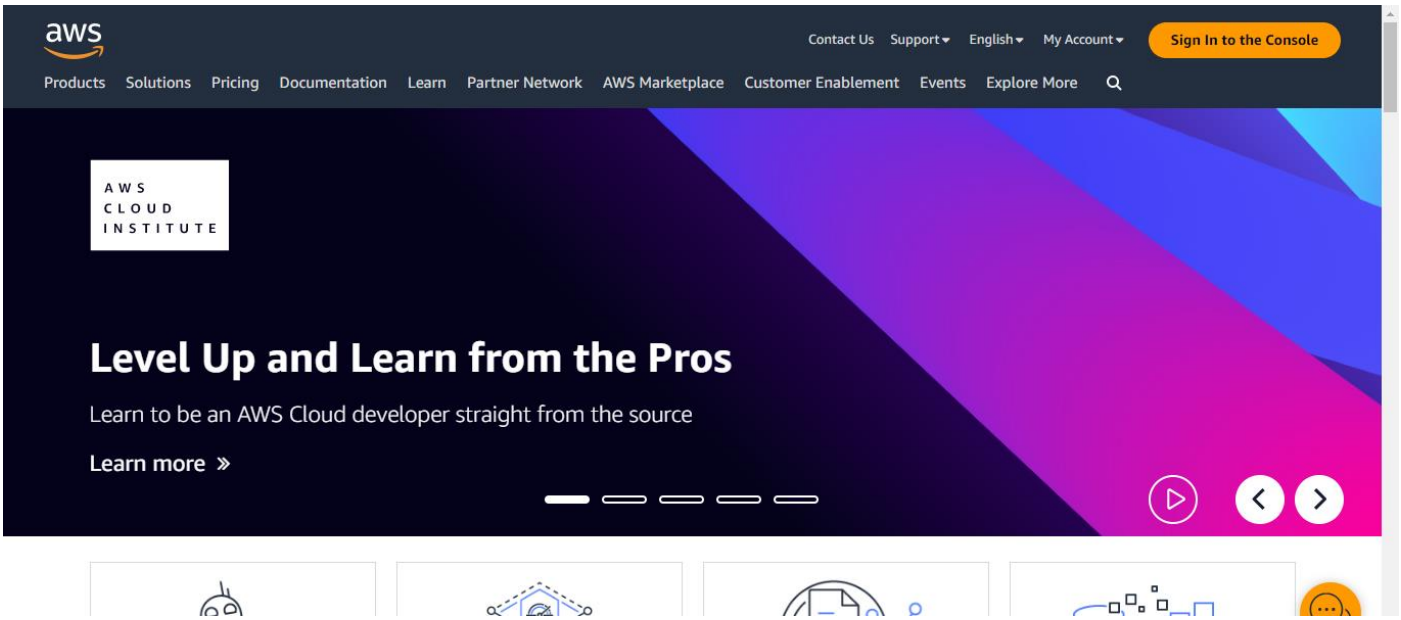
一、Forward

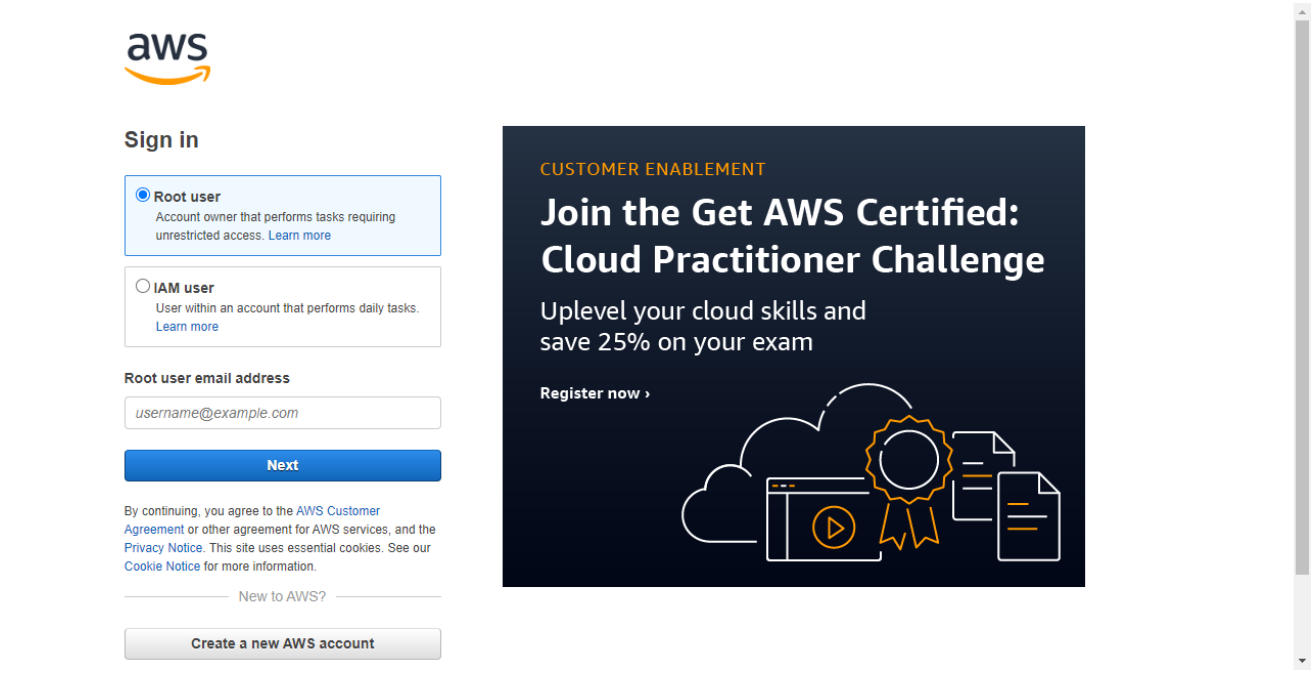
Currently, some customers will connect to Amazon AWS platform through MQTT protocol based on Quectel module; This document is aimed at the Quectel's module access to the AWS platform and the use of MQTT application so that customers or other-relevant can understand docking methods and processes on the platform and module in a quick and high-effective way.

二、Login to AWS

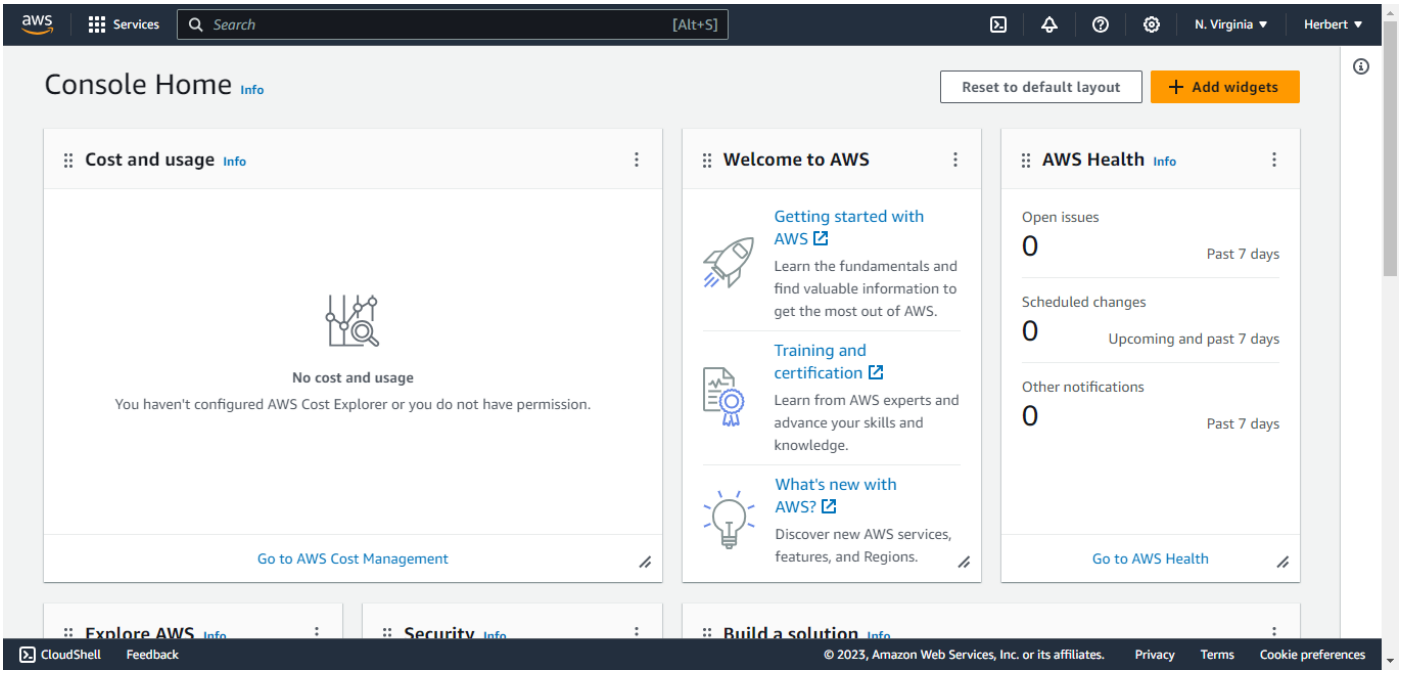
AWS Platform：https://aws.amazon.com/?nc1=h_ls

By the applied login account, click "Sigin In to the Console" to login and enter the home page of the console, as shown below;

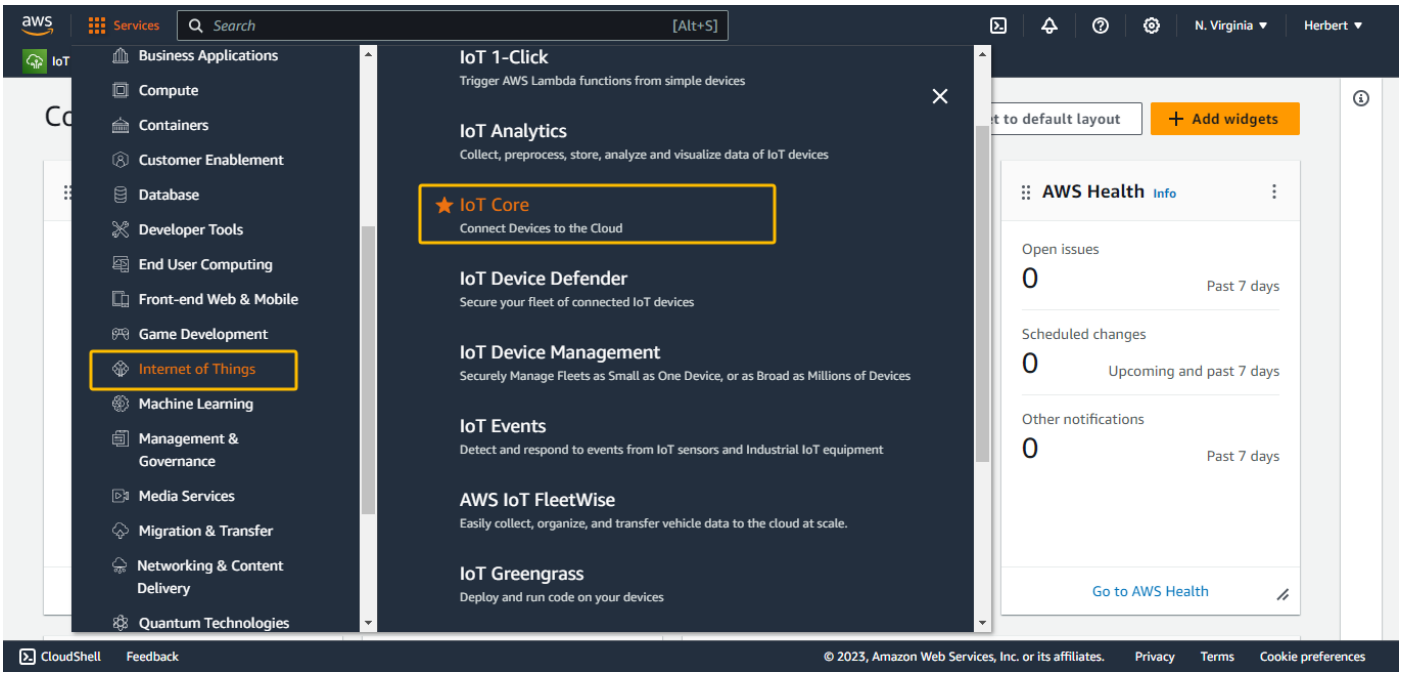


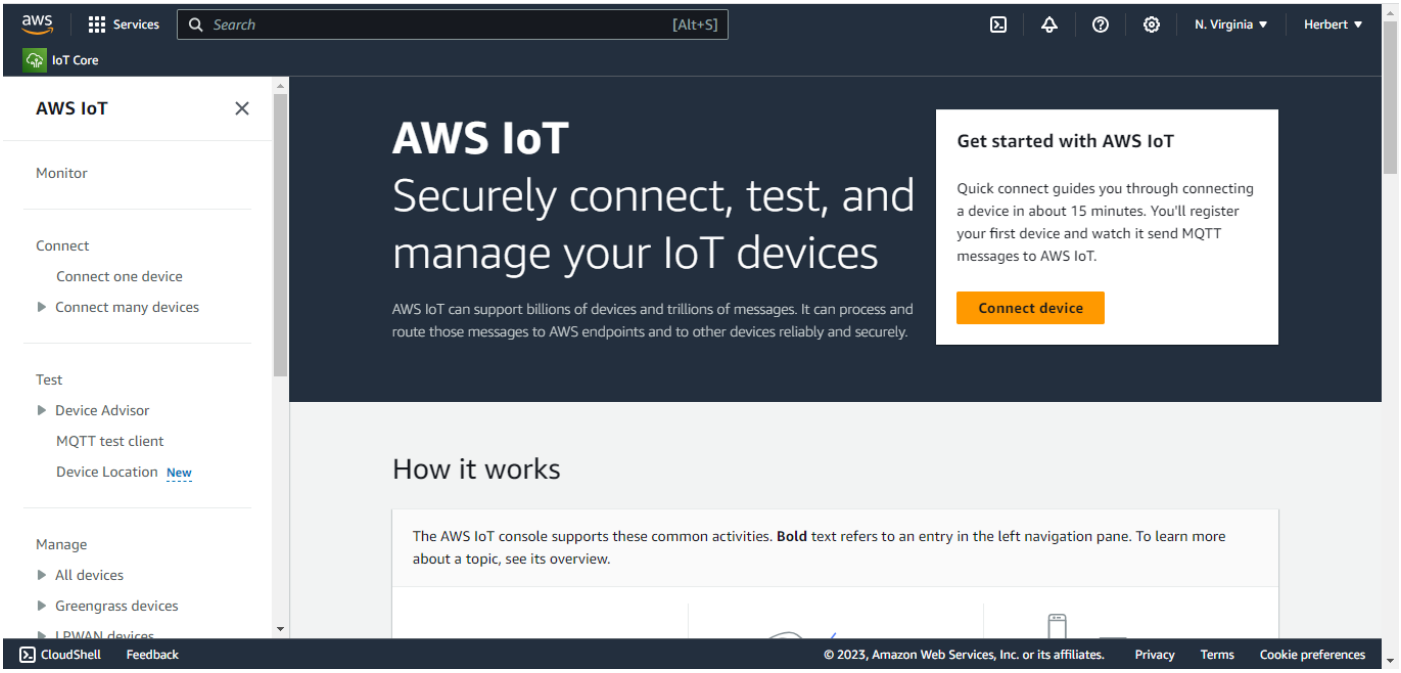


AWS control console：https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1



Click "Services → Internet of Things → IoT Core" to enter the home page of AWS IoT,as shown below.

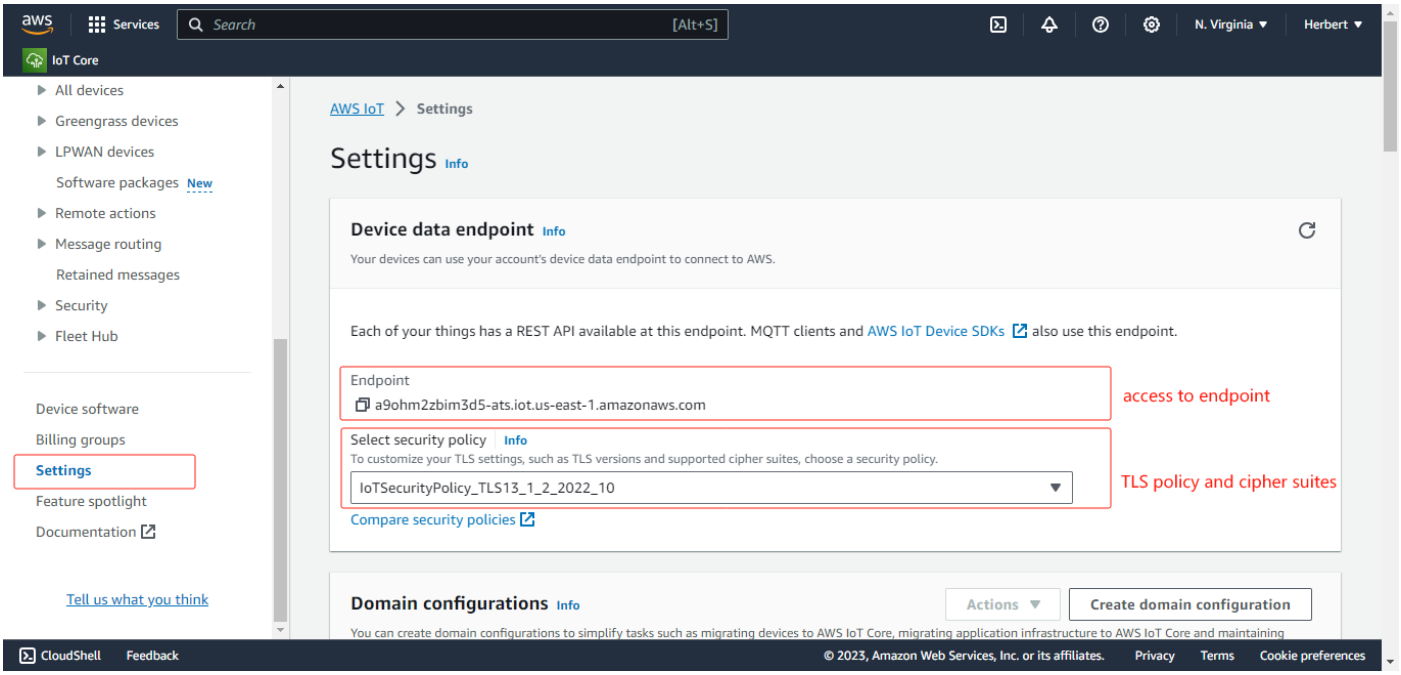




三、AWS IoT Platform Settings

3.1 Device Data Endpoint

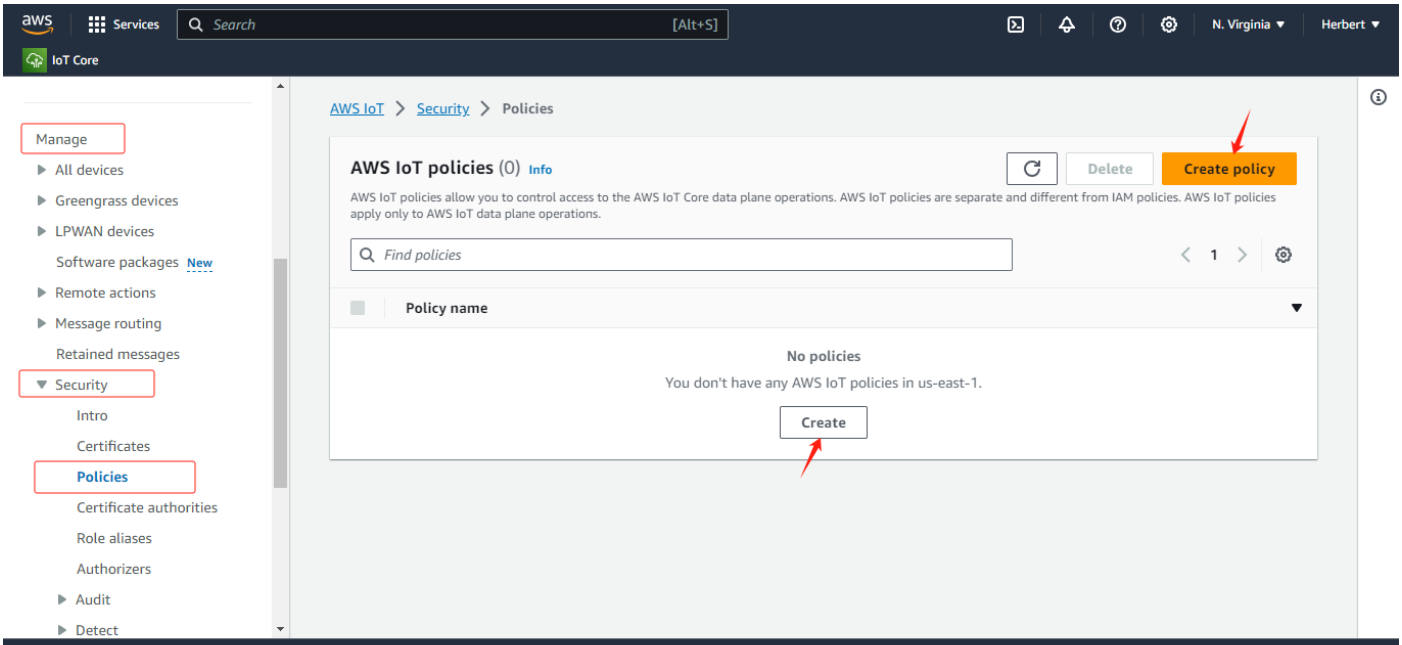
As shown below, you can access the Settings page through "Settings" in the control panel on the left side of the AWS IoT page, view the device data endpoint to be accessed and select a security policy (note that the security policy is associated with the cipher suites,so you need to select the cipher suite and security policy supported by the module).

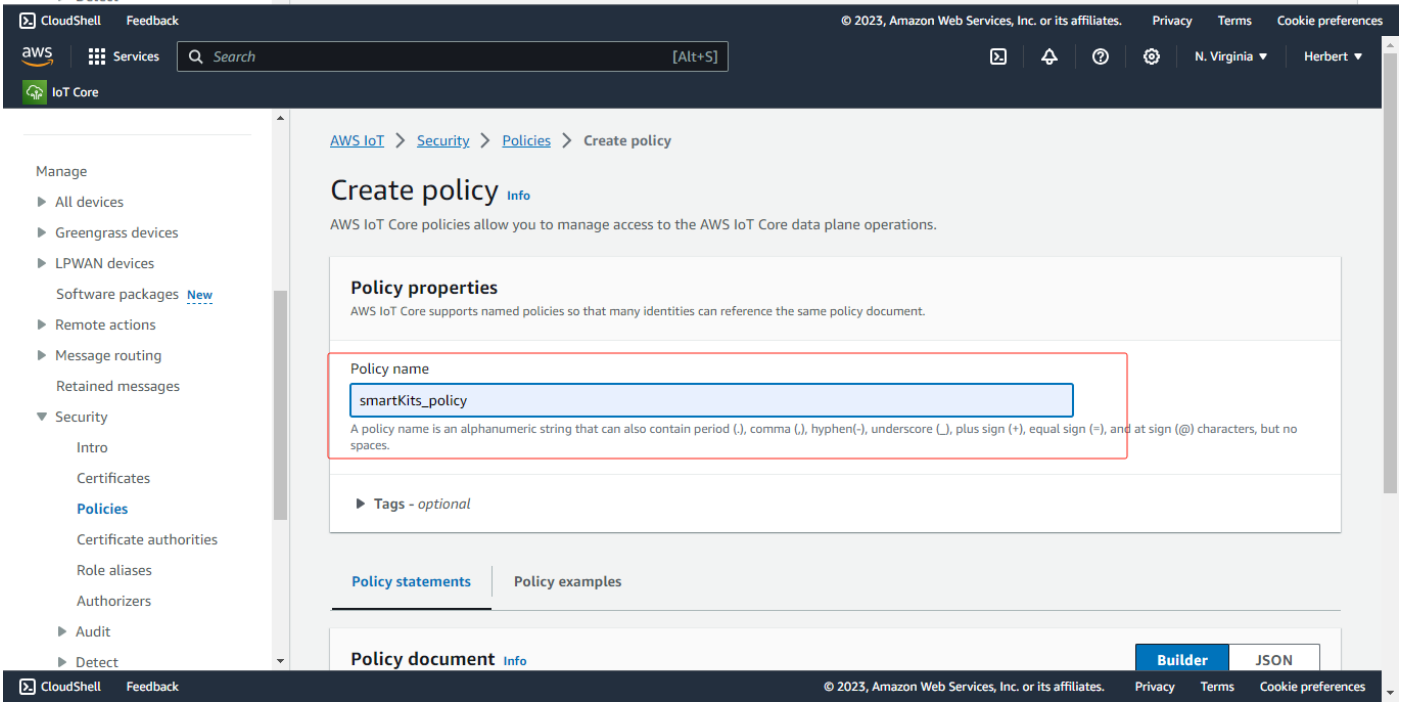


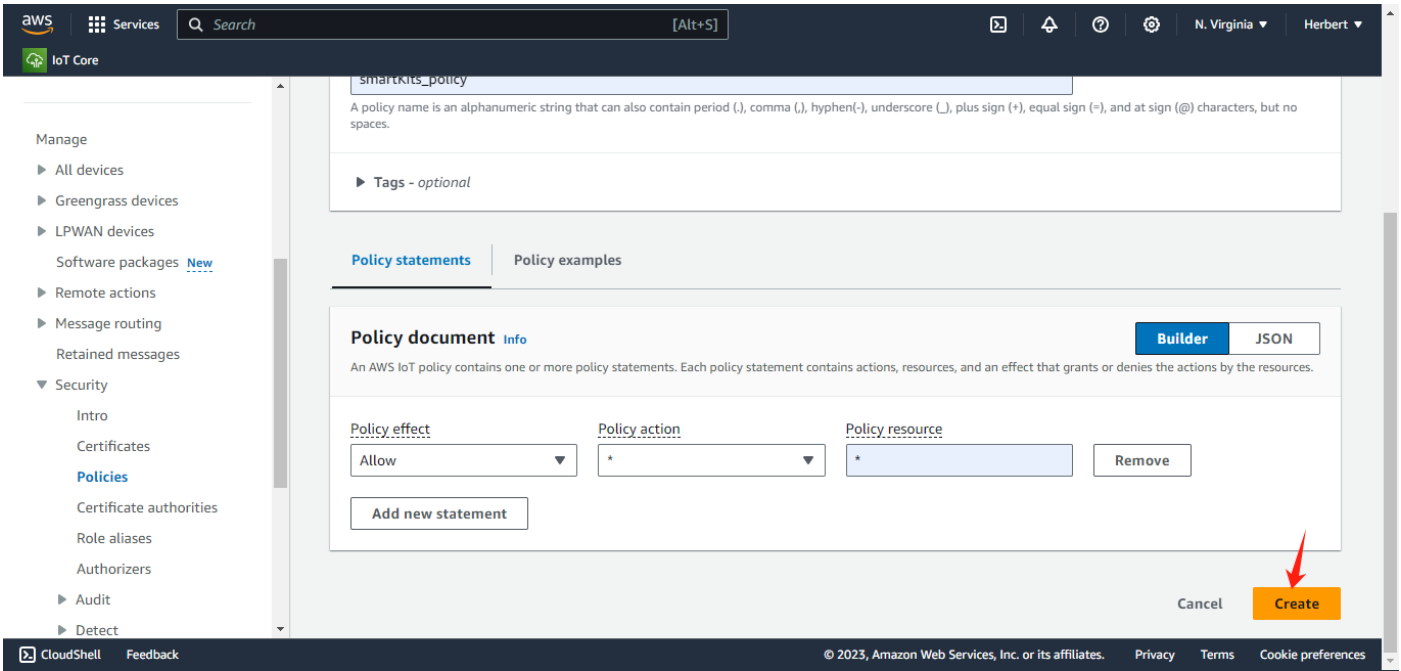
3.2 AWS IoT Policies

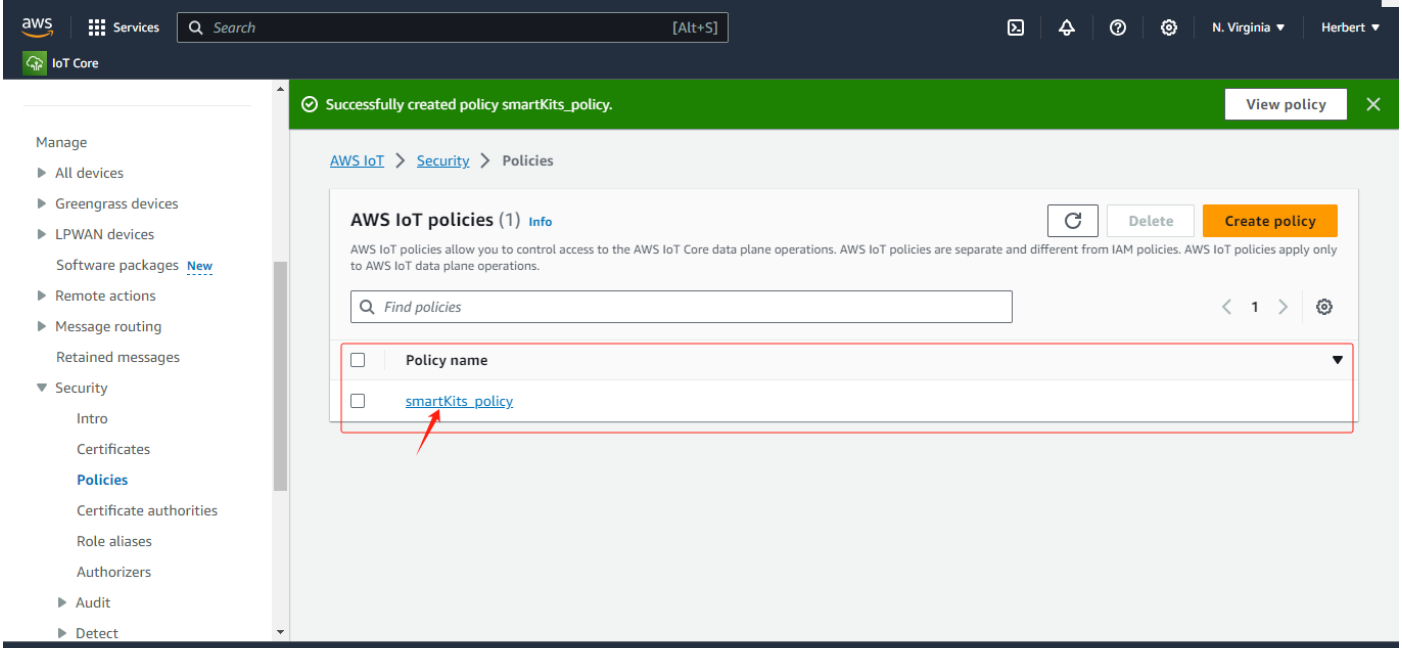
As shown below, to enter the policy configuration page through "Manage → Security → Policies" in the control panel

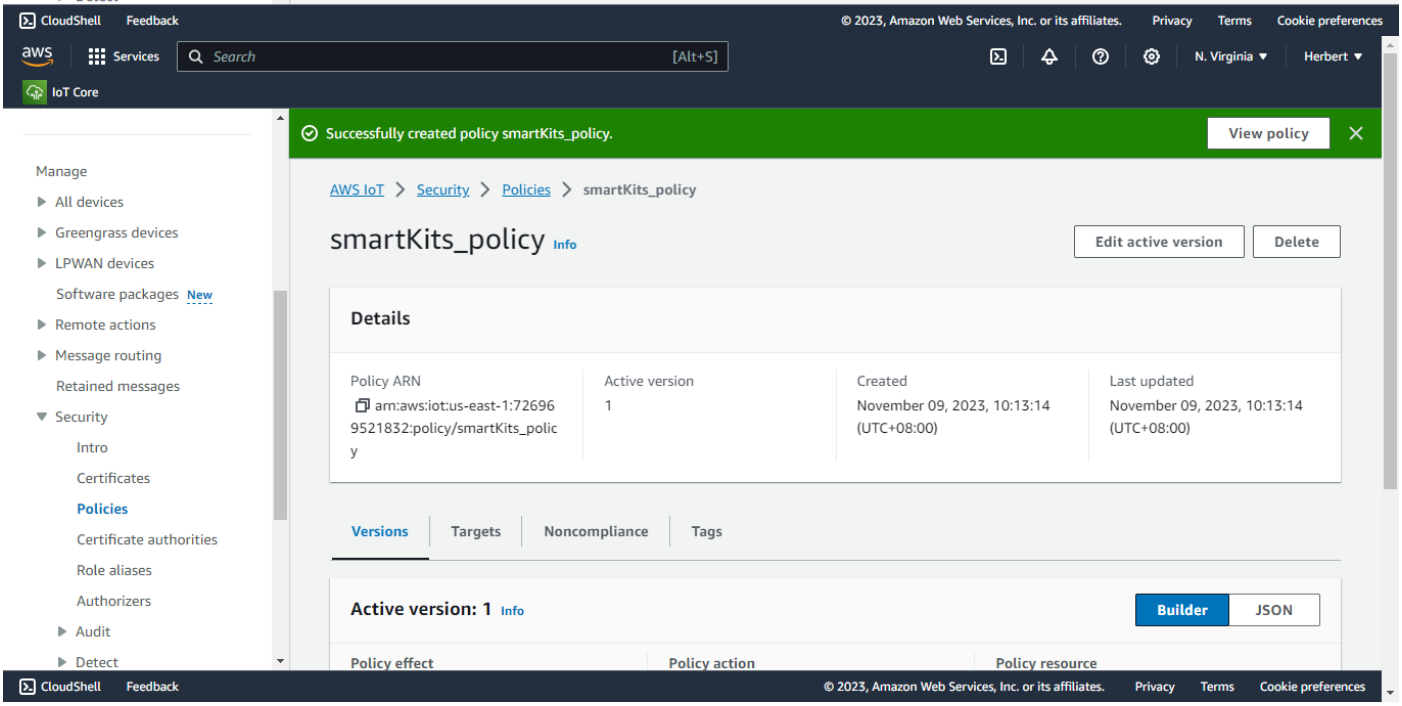
on the left side of the AWS IoT page, click "Create Policy", and configure related policy attributes. In the policy statement, set Policy Effect to Allow, Policy Action to * (all AWS IoT operations), and Policy Resource to *.





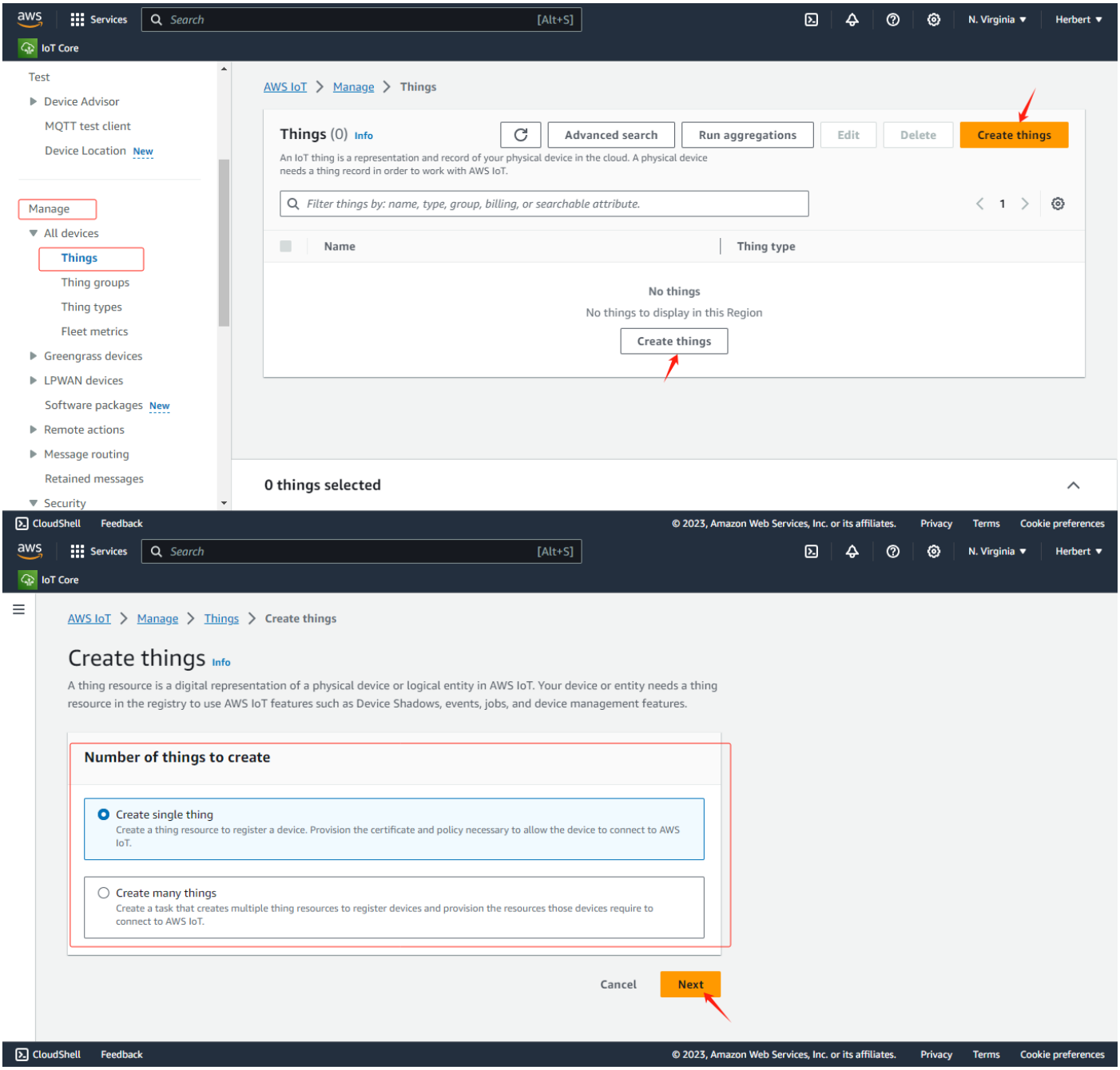

aws
Services
Search
[Alt+S]
N. Virginia
Herbert
IoT Core
smartKits_policy
A policy name is an alphanumeric string that can also contain period (.), comma (,), hyphen(-), underscore (_), plus sign (+), equal sign (=), and at sign (@) characters, but no spaces.
Tags - optional
Policy statements
Policy examples
Policy document Info
Builder
JSON
An AWS IoT policy contains one or more policy statements. Each policy statement contains actions, resources, and an effect that grants or denies the actions by the resources.
Policy effect
Policy action
Policy resource
Allow
*
*
Remove
Add new statement
Cancel
Create
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Manage
All devices
Greengrass devices
LPWAN devices
Software packages New
Remote actions
Message routing
Retained messages
Security
Intro
Certificates
Policies
Certificate authorities
Role aliases
Authorizers
Audit
Detect

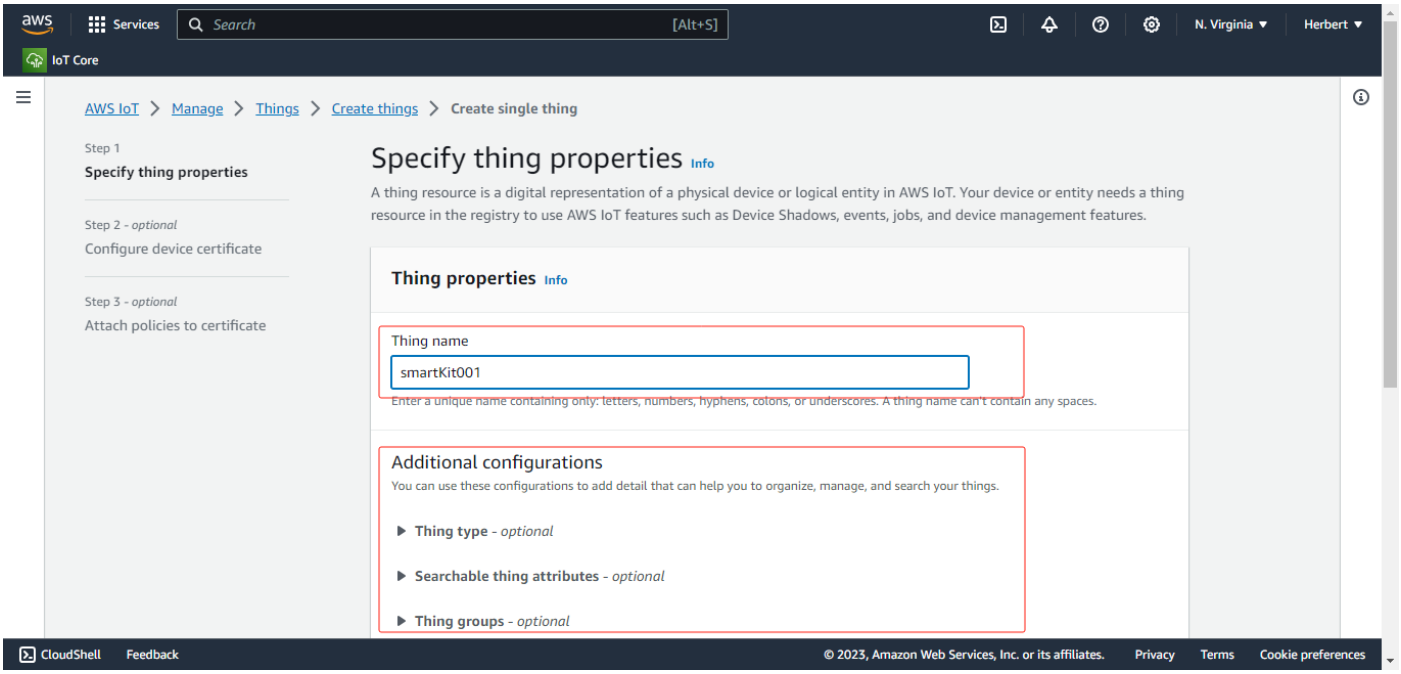

Successfully created policy smartKits_policy.
View policy
AWS IoT > Security > Policies
AWS IoT policies (1) Info
Delete
Create policy
AWS IoT policies allow you to control access to the AWS IoT Core data plane operations. AWS IoT policies are separate and different from IAM policies. AWS IoT policies apply only to AWS IoT data plane operations.
Find policies
1
Policy name
smartKits_policy


Successfully created policy smartKits_policy.
View policy
AWS IoT > Security > Policies > smartKits_policy
smartKits_policy Info
Edit active version
Delete
Details
Policy ARN
arn:aws:iot:us-east-1:726969521832:policy/smartKits_policy
Active version
1
Created
November 09, 2023, 10:13:14 (UTC+08:00)
Last updated
November 09, 2023, 10:13:14 (UTC+08:00)
Versions
Targets
Noncompliance
Tags
Active version: 1 Info
Builder
JSON
Policy effect
Policy action
Policy resource

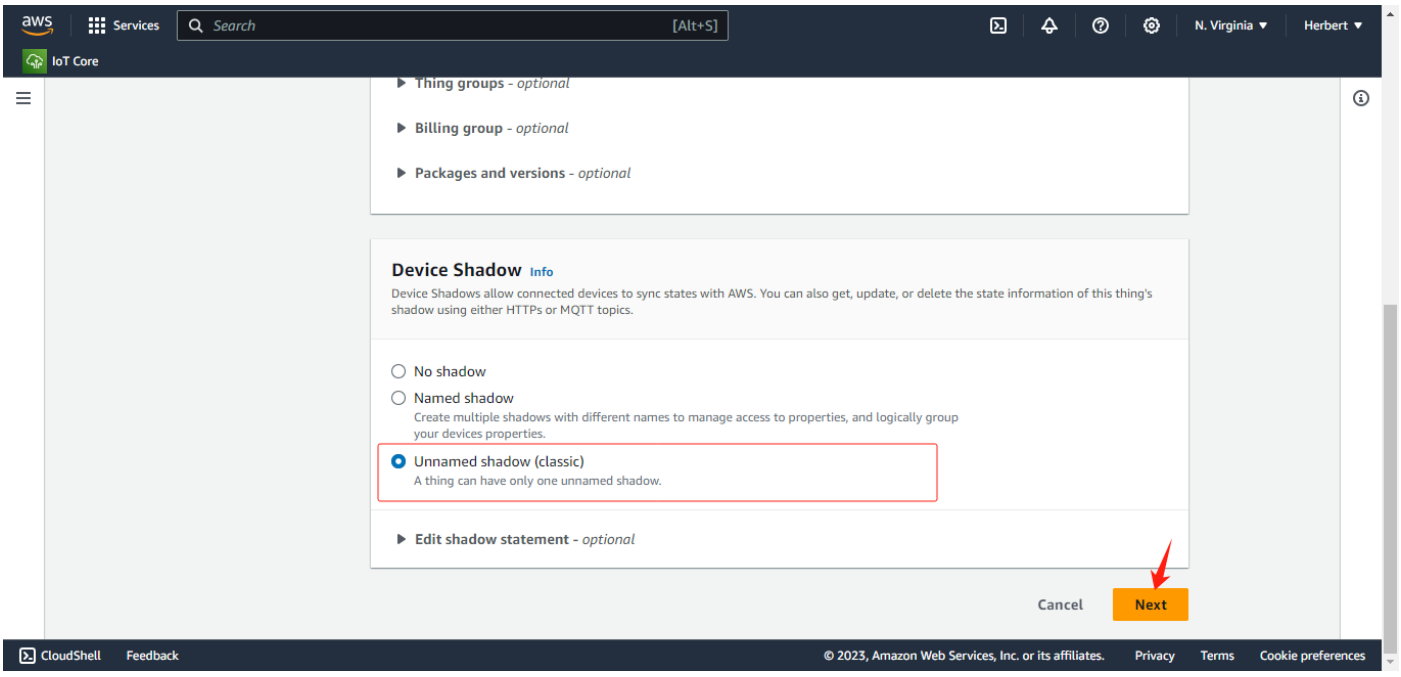
3.3 Add Tings

Go to the Add/create things by "Manage → All devices → Things" in the control panel on the left side of the AWS IoT page, click "Create things", and create a single thing or multiple things according to actual requirements; Take the following example of smartKit001, and then fill in and select the specified things properties (optional); to select other configurations based on actual application requirements, as shown below.

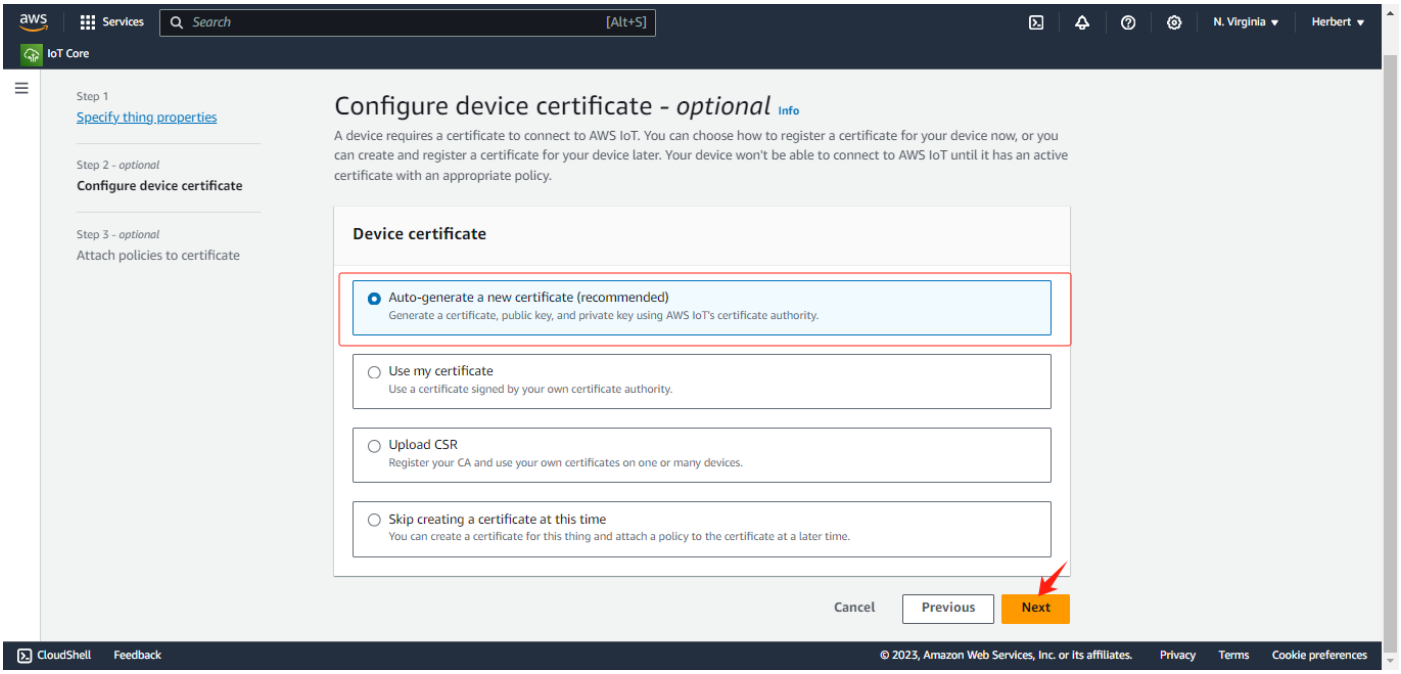




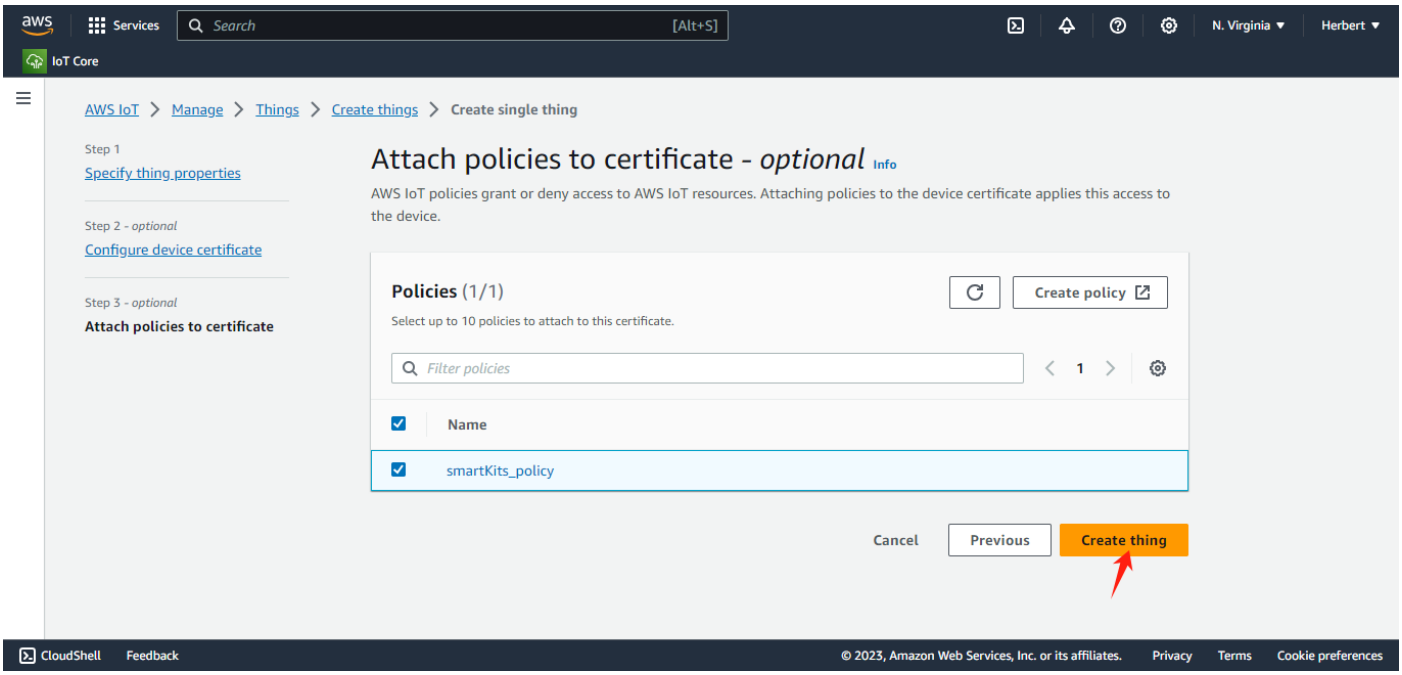
Select whether to add "Device Shadow" according to the actual application requirements.To facilitate subsequent debugging, currently select "Unnamed Shadow (Classic)";



You need to configure the device certificate based on the different mode of certificate. Let's take “Auto-Generate a New certificate(recommended)” as an example.



Attach a policy to the current thing, select the policy created above, and obtain the relevant certificate; As shown below;

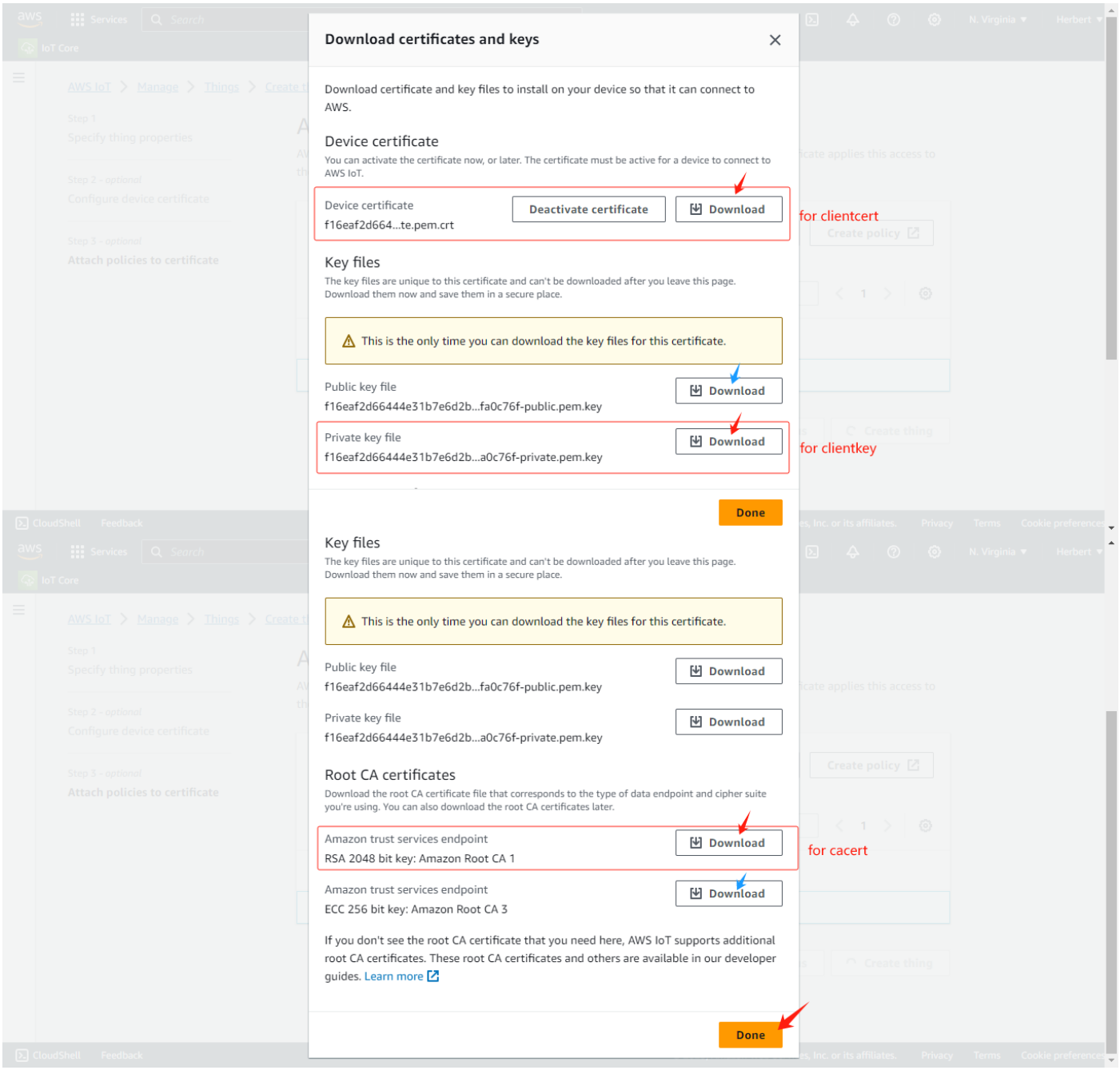


On the "Download Certificates and Keys" page, download the CA certificate and key files automatically generated by the platform and save it.

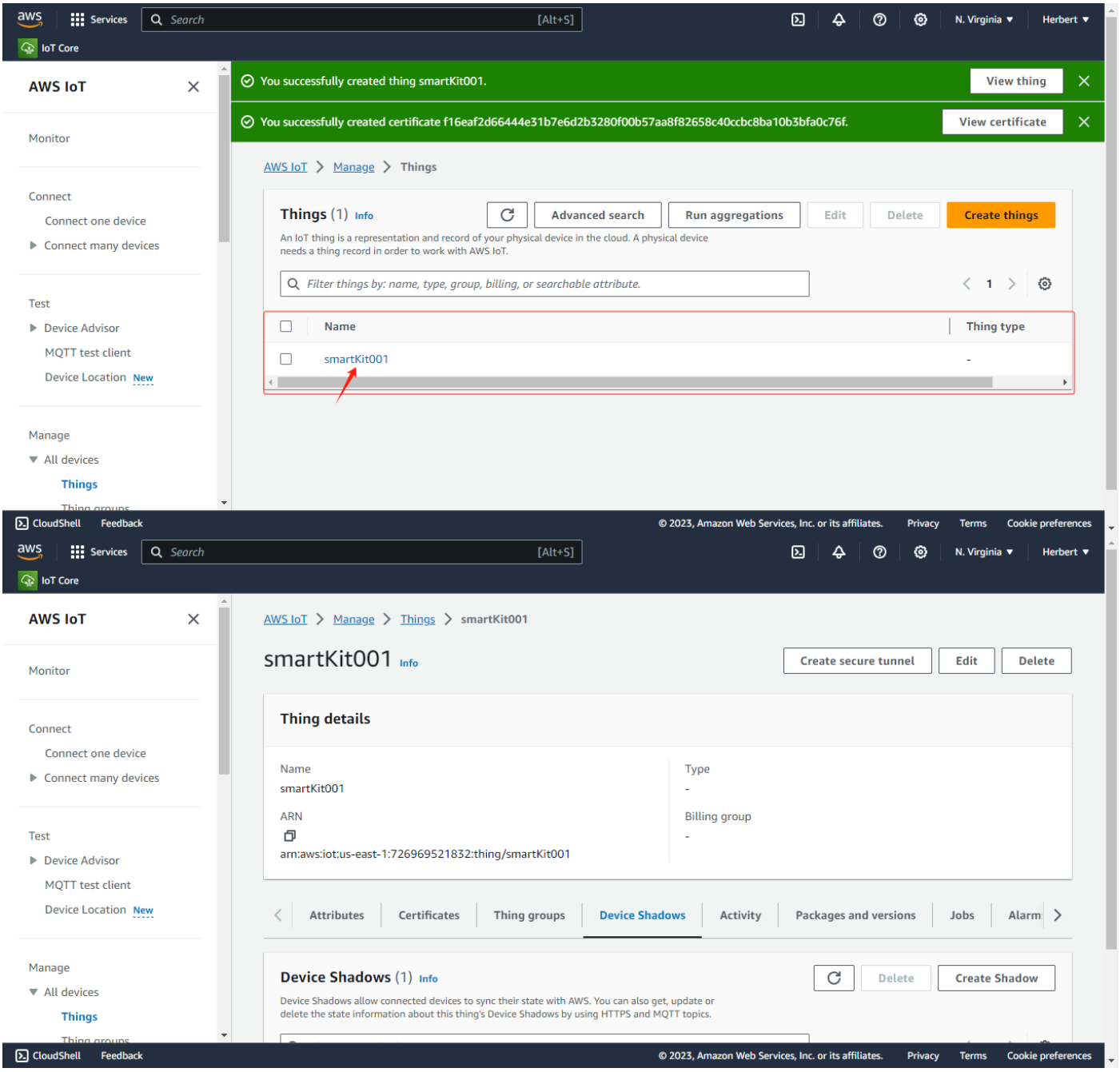
xxxxxxxxxx-certificate.pem for clientcert（Client Certificate File）;

xxxxxxxxxx-private.pem for clientkey（Client Key File）;

AmazonRootCA1.pem for cacert（CA File）

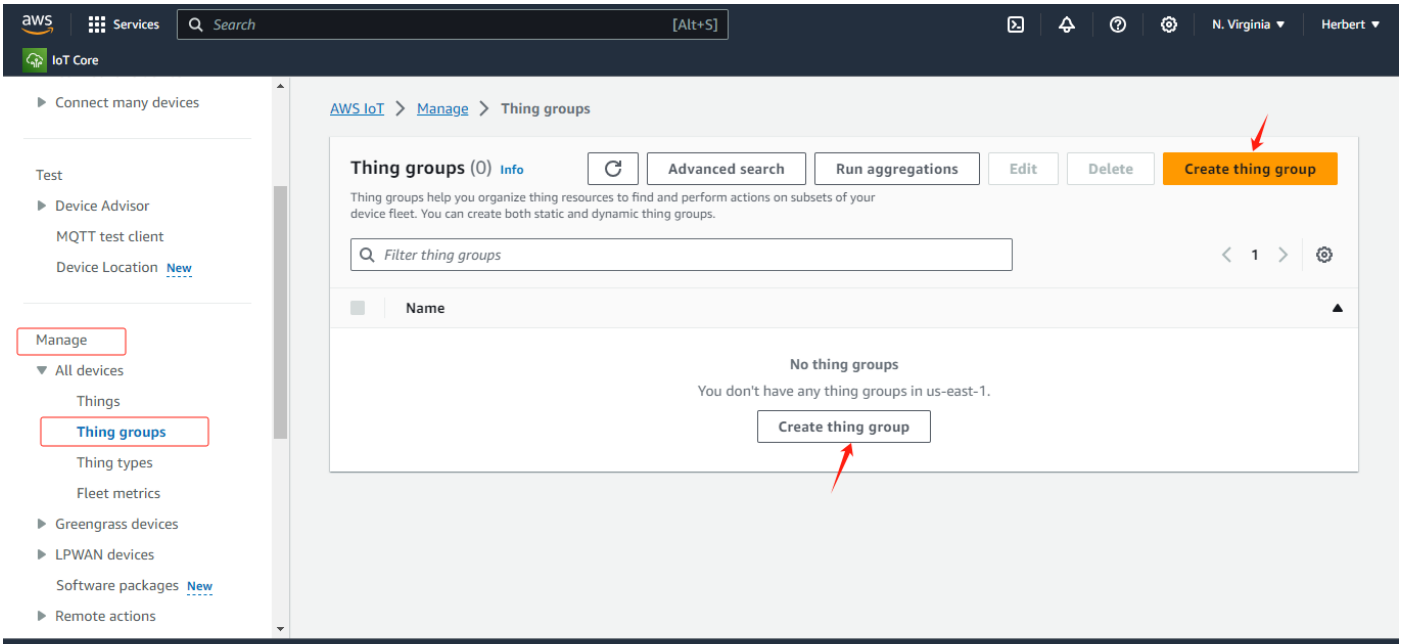


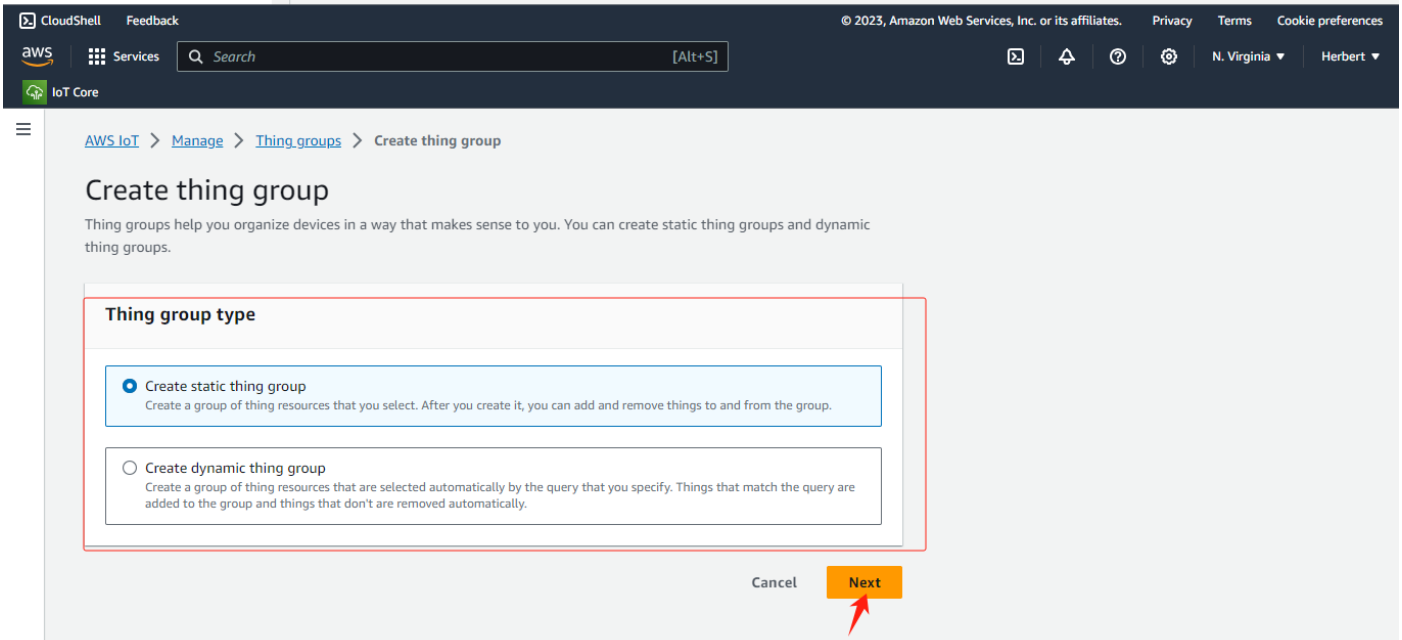
You can click "smartKit001" to view the thing details;

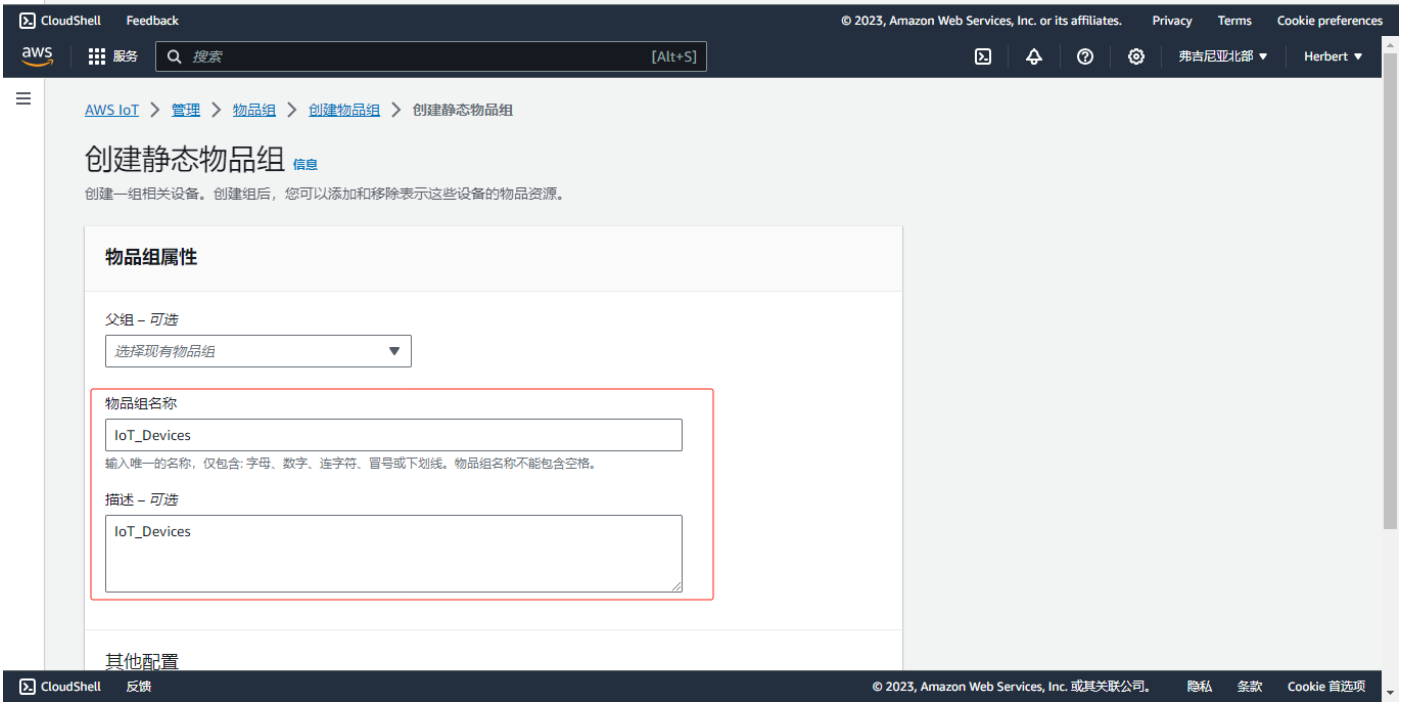


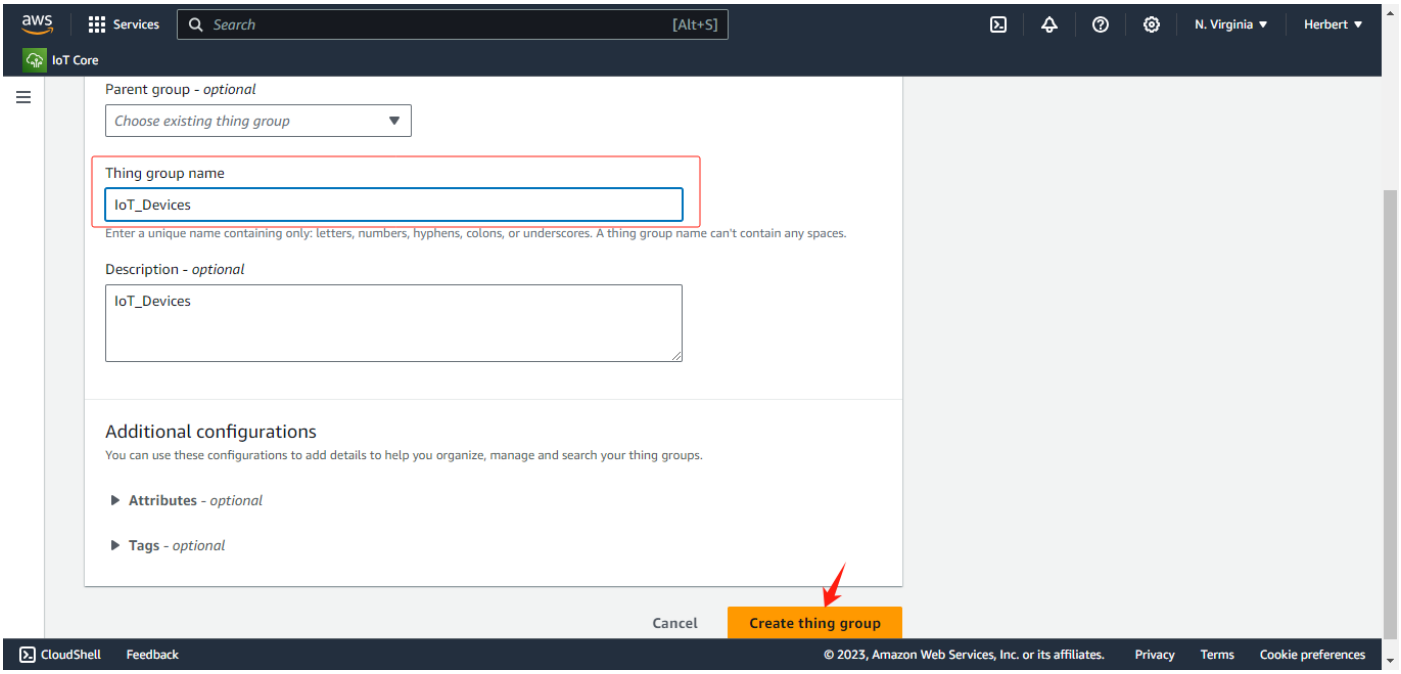
3.4 Add Ting Groups(Options)

As shown in the figure below, you can enter the thing groups configuration page through "Manage → All Devices → thing Groups" in the control panel on the left side of the AWS IoT, click "Create thing Group",then to select the thing group type, fill in the corresponding the name of thing group, and configure other options according to requirements, and then to click "Create thing Group".

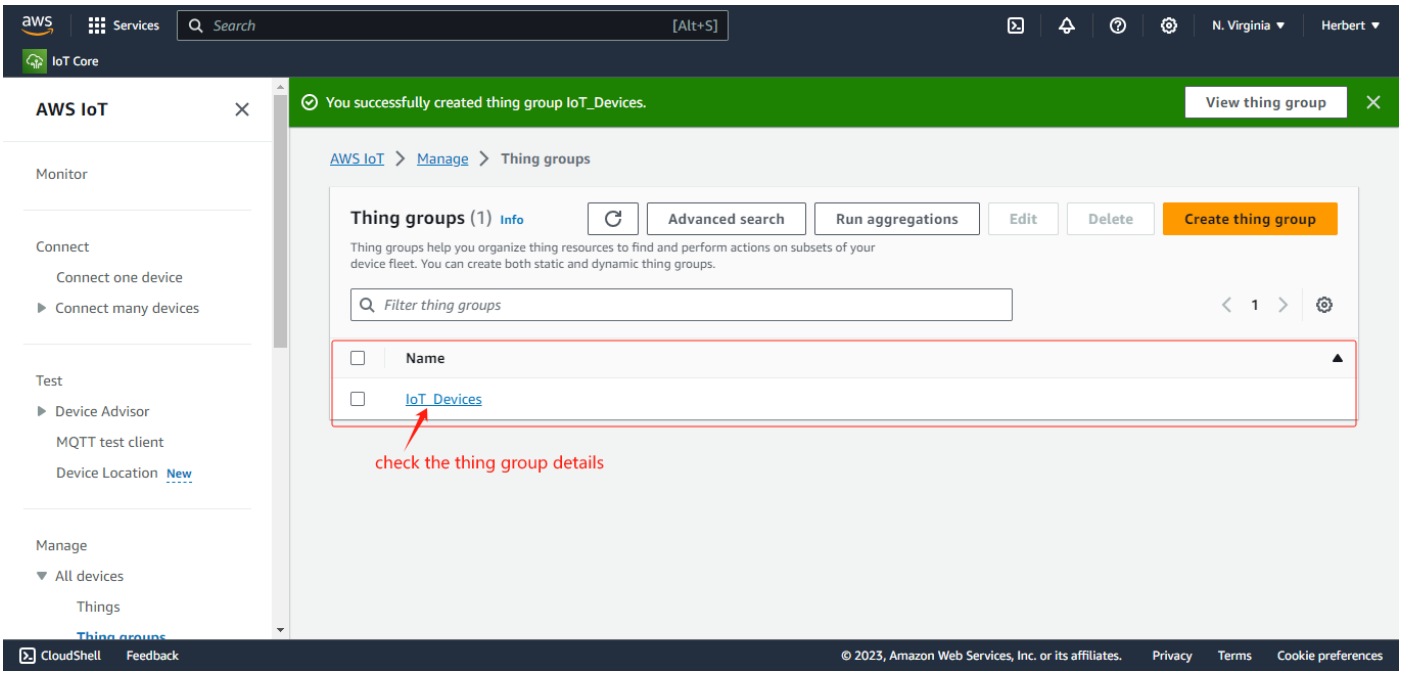

Services
Search
[Alt+S]
N. Virginia
Herbert
IoT Core
Connect many devices
Test
Device Advisor
MQTT test client
Device Location New
Manage
All devices
Things
Thing groups
Thing types
Fleet metrics
Greengrass devices
LPWAN devices
Software packages New
Remote actions
AWS IoT > Manage > Thing groups
Thing groups (0) Info
Advanced search
Run aggregations
Edit
Delete
Create thing group
Thing groups help you organize thing resources to find and perform actions on subsets of your device fleet. You can create both static and dynamic thing groups.
Filter thing groups
Name
No thing groups
You don't have any thing groups in us-east-1.
Create thing group

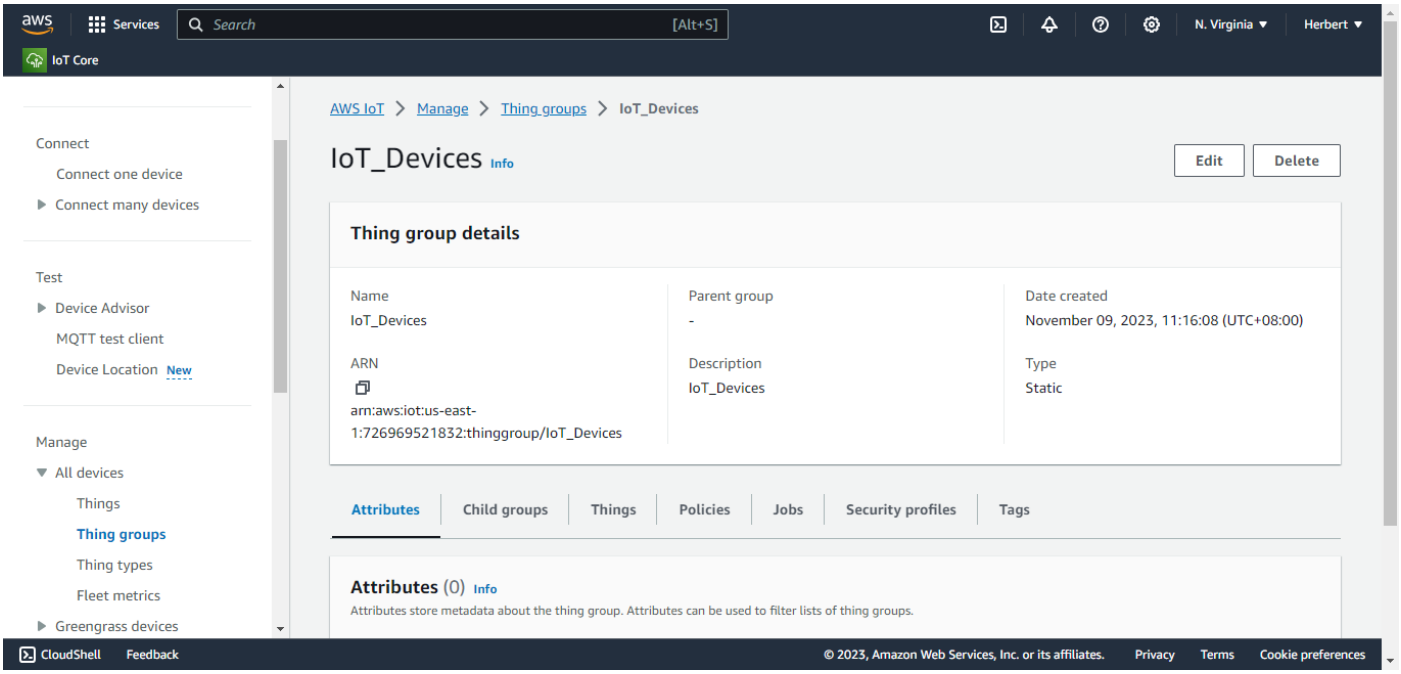

CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Services
Search
[Alt+S]
N. Virginia
Herbert
IoT Core
AWS IoT > Manage > Thing groups > Create thing group
Create thing group
Thing groups help you organize devices in a way that makes sense to you. You can create static thing groups and dynamic thing groups.
Thing group type
Create static thing group
Create a group of thing resources that you select. After you create it, you can add and remove things to and from the group.
Create dynamic thing group
Create a group of thing resources that are selected automatically by the query that you specify. Things that match the query are added to the group and things that don't are removed automatically.
Cancel
Next


CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
服务
搜索
[Alt+S]
弗吉尼亚北部
Herbert
AWS IoT > 管理 > 物品组 > 创建物品组 > 创建静态物品组
创建静态物品组 信息
创建一组相关设备。创建组后，您可以添加和移除表示这些设备的物品资源。
物品组属性
父组 – 可选
选择现有物品组
物品组名称
IoT_Devices
输入唯一的名称，仅包含: 字母、数字、连字符、冒号或下划线。物品组名称不能包含空格。
描述 – 可选
IoT_Devices
其他配置
CloudShell
反馈
© 2023, Amazon Web Services, Inc. 或其关联公司。
隐私
条款
Cookie 首选项

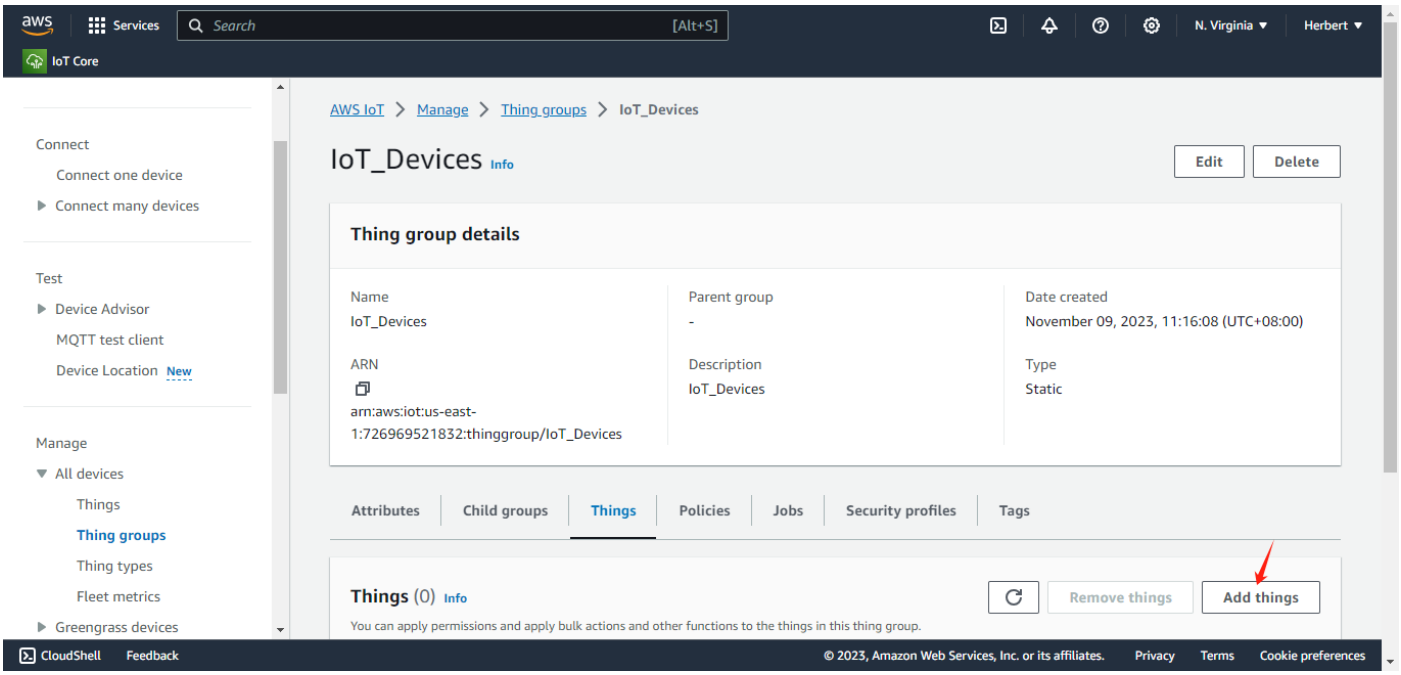


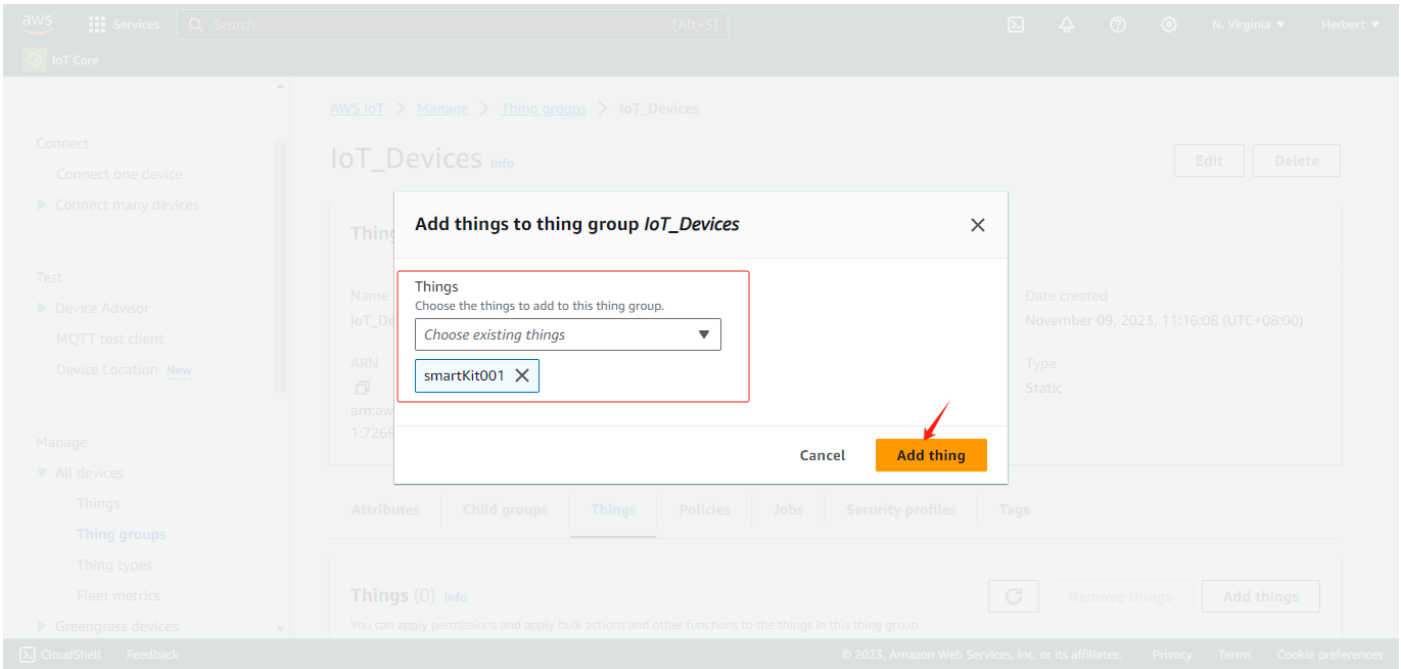
Click on the created thing group to view the details, as shown below;

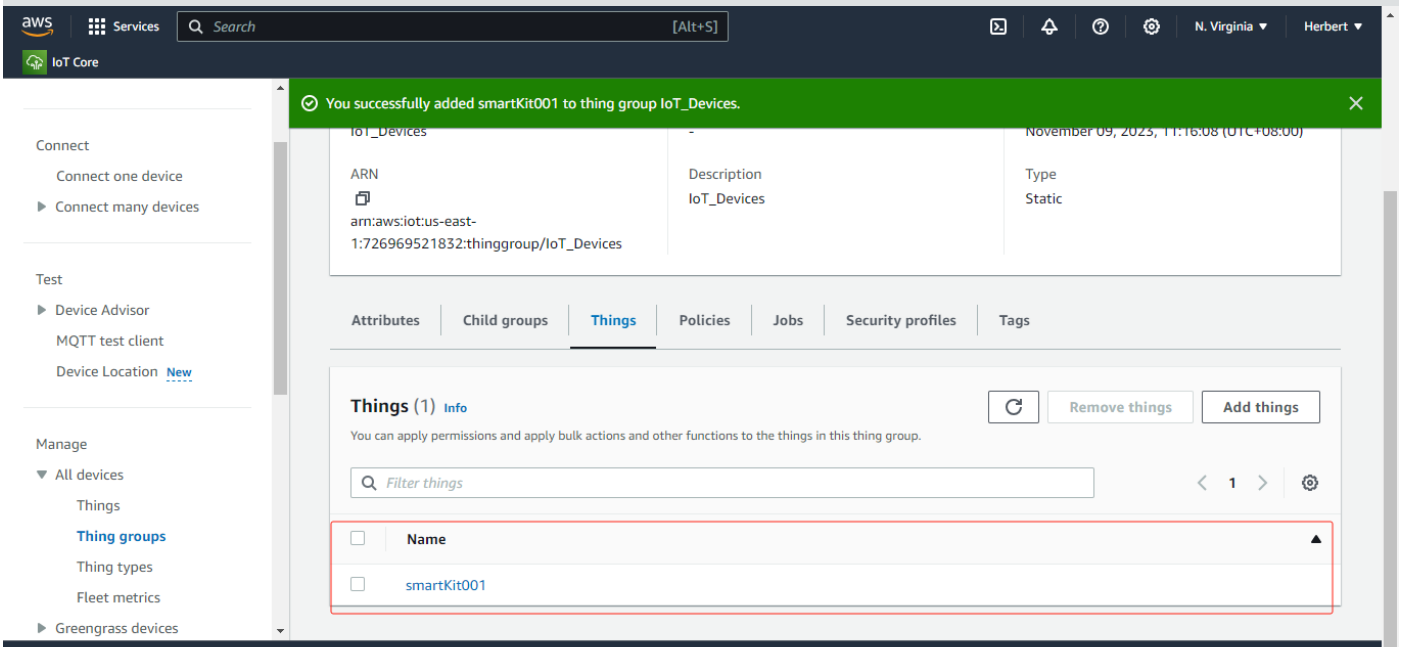


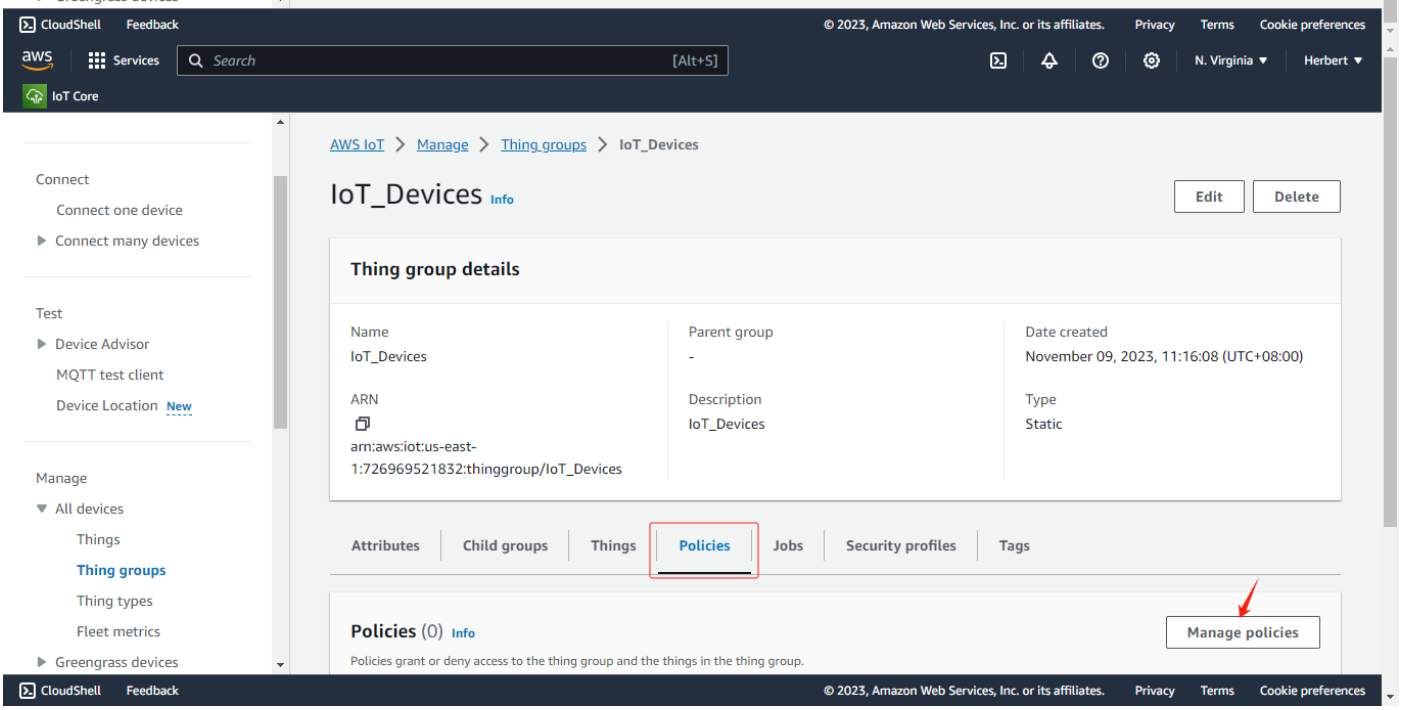


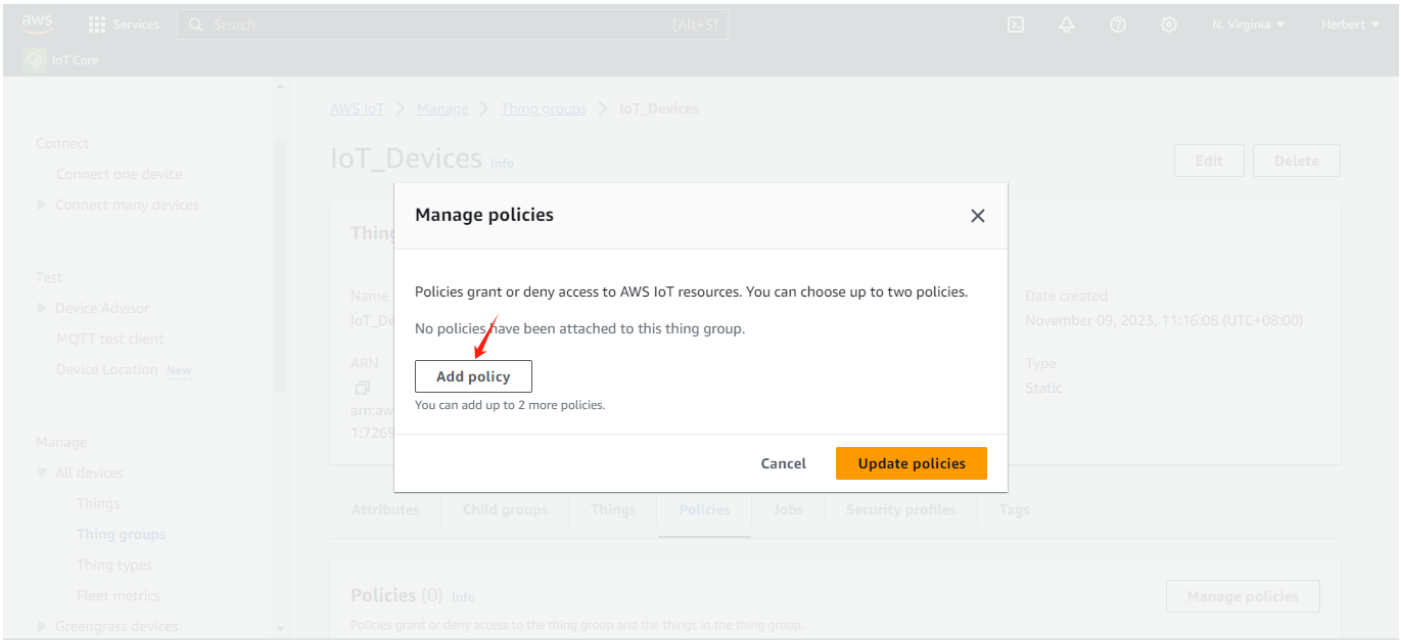
By the configuration item in the thing group details, you can associate the above created "Policies" and "Things", as shown in the following figure;

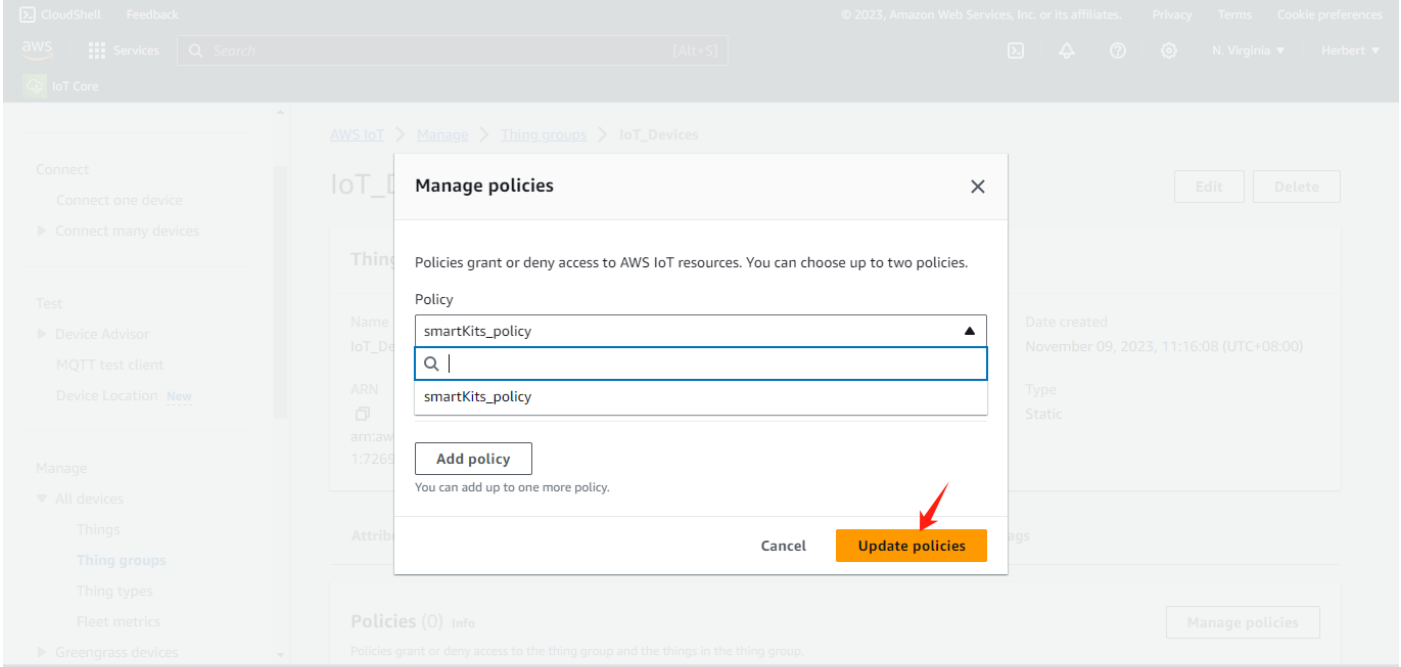


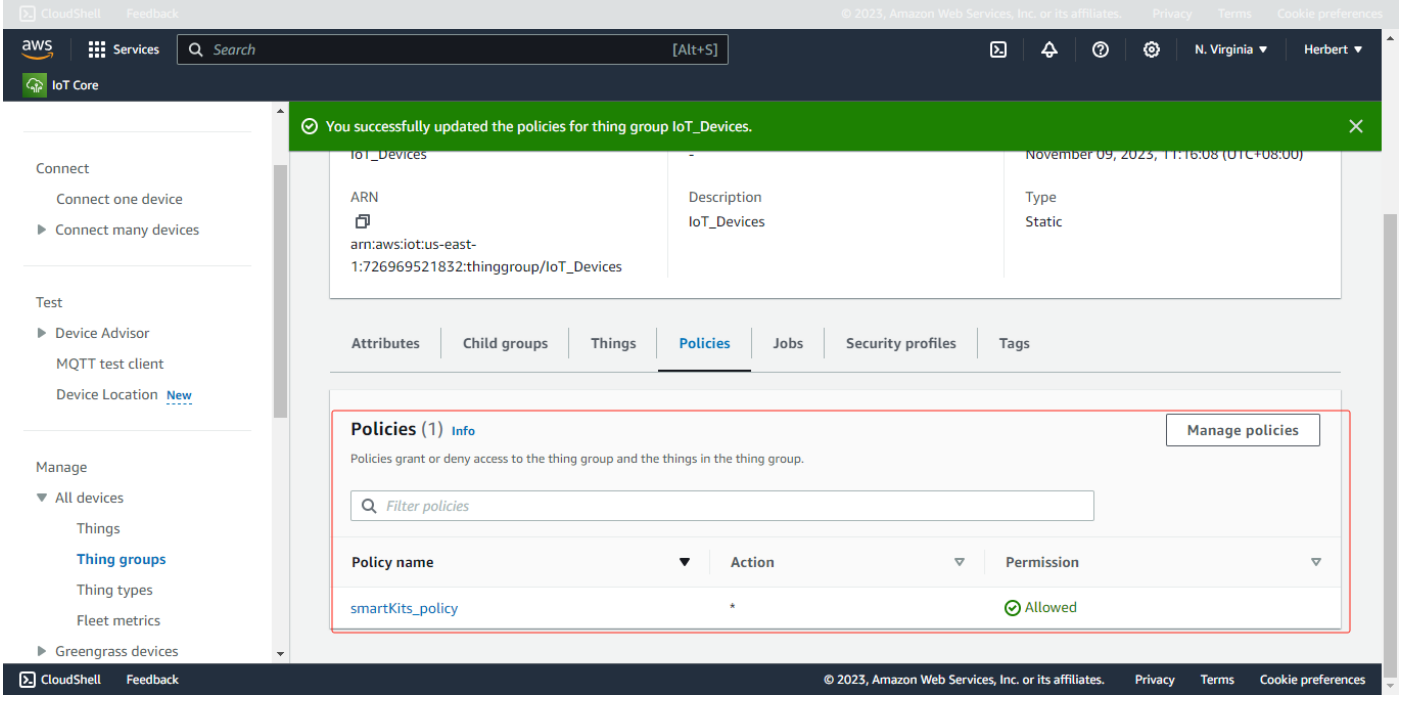

Add things to thing group IoT_Devices
Things
Choose the things to add to this thing group.
Choose existing things
smartKit001
Cancel
Add thing


You successfully added smartKit001 to thing group IoT_Devices.
ARN
arn:aws:iot:us-east-1:726969521832:thinggroup/IoT_Devices
Description
IoT_Devices
Type
Static
Attributes
Child groups
Things
Policies
Jobs
Security profiles
Tags
Things (1) Info
You can apply permissions and apply bulk actions and other functions to the things in this thing group.
Remove things
Add things
Filter things
Name
smartKit001


AWS IoT > Manage > Thing groups > IoT_Devices
IoT_Devices Info
Edit
Delete
Thing group details
Name
IoT_Devices
Parent group
-
Date created
November 09, 2023, 11:16:08 (UTC+08:00)
ARN
arn:aws:iot:us-east-1:726969521832:thinggroup/IoT_Devices
Description
IoT_Devices
Type
Static
Attributes
Child groups
Things
Policies
Jobs
Security profiles
Tags
Policies (0) Info
Policies grant or deny access to the thing group and the things in the thing group.
Manage policies


Manage policies
Policies grant or deny access to AWS IoT resources. You can choose up to two policies.
No policies have been attached to this thing group.
Add policy
You can add up to 2 more policies.
Cancel
Update policies


Manage policies
Policies grant or deny access to AWS IoT resources. You can choose up to two policies.
Policy
smartKits_policy
smartKits_policy
Add policy
You can add up to one more policy.
Cancel
Update policies

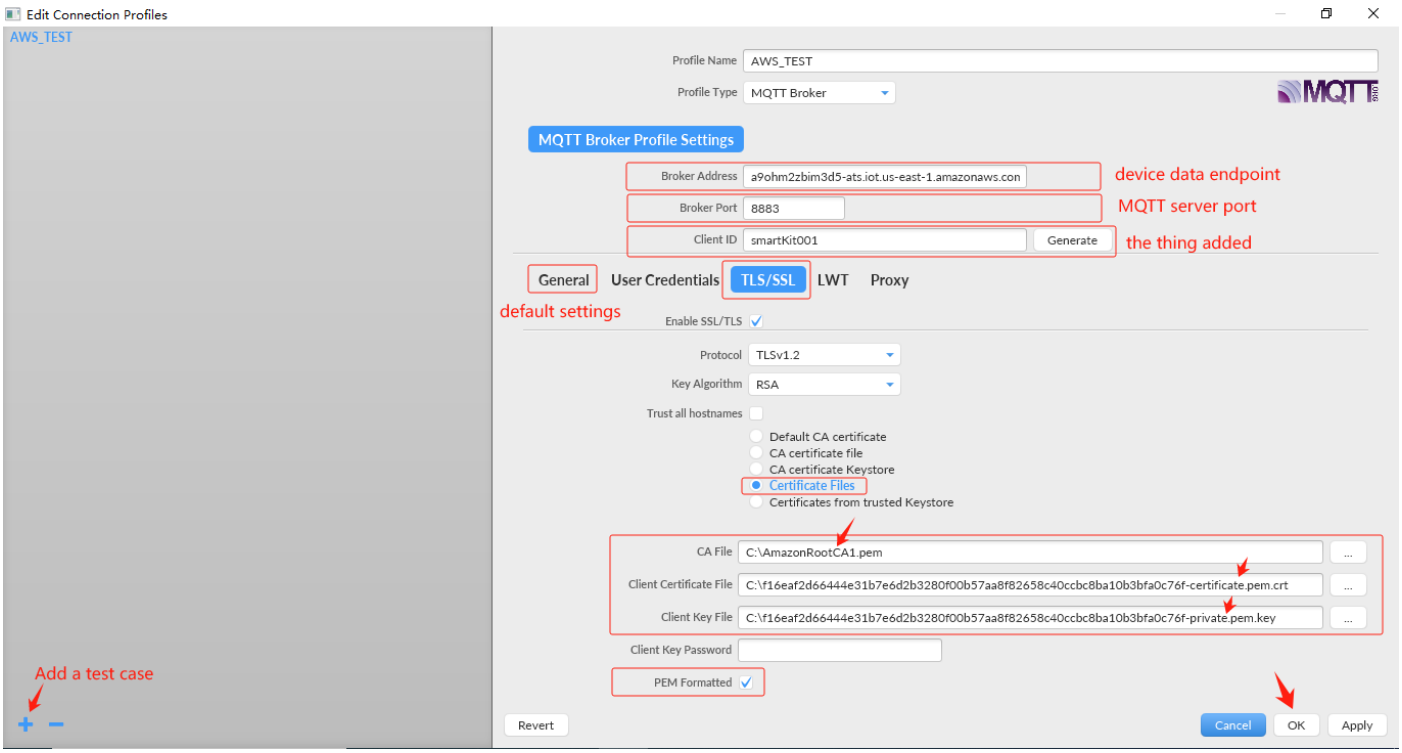

You successfully updated the policies for thing group IoT_Devices.
ARN
arn:aws:iot:us-east-1:726969521832:thinggroup/IoT_Devices
Description
IoT_Devices
Type
Static
Attributes
Child groups
Things
Policies
Jobs
Security profiles
Tags
Policies (1) Info
Manage policies
Policies grant or deny access to the thing group and the things in the thing group.
Filter policies
Policy name
Action
Permission
smartKits_policy
*
Allowed

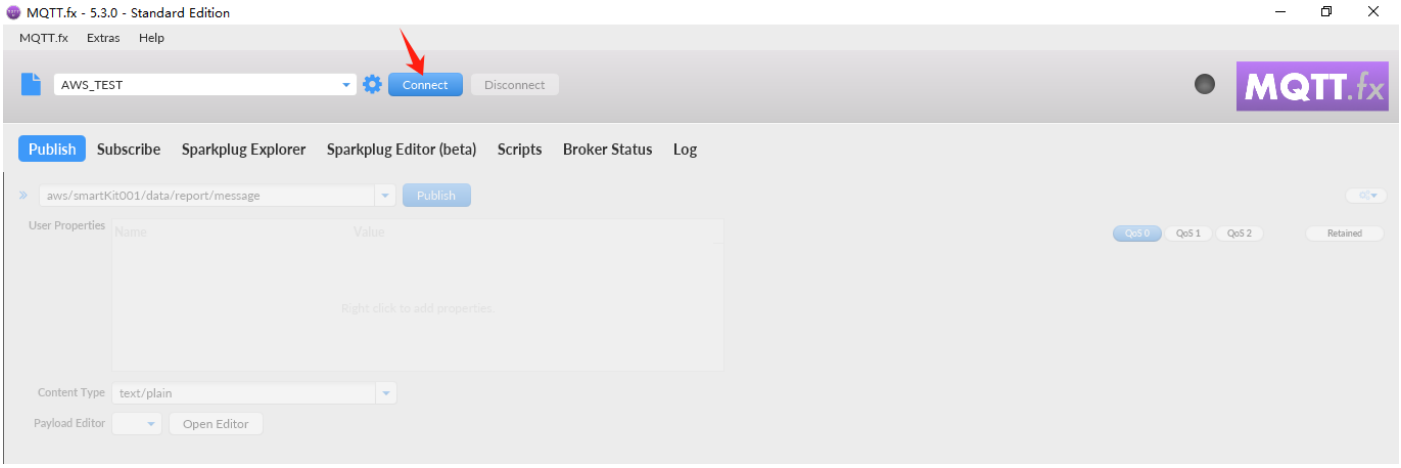
四、MQTT Test

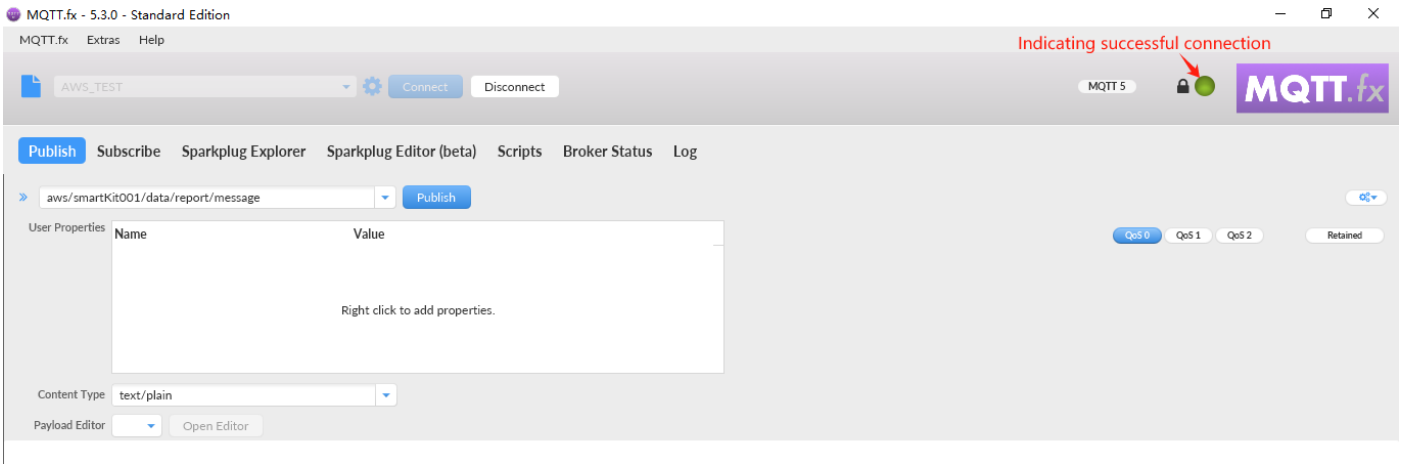
4.1 MQTT.fx Configuration and Access to AWS IoT

The following tests are based on the MQTT.fx tool： https://softblade.de/en/download-2/;

the detailed configuration as shown below；

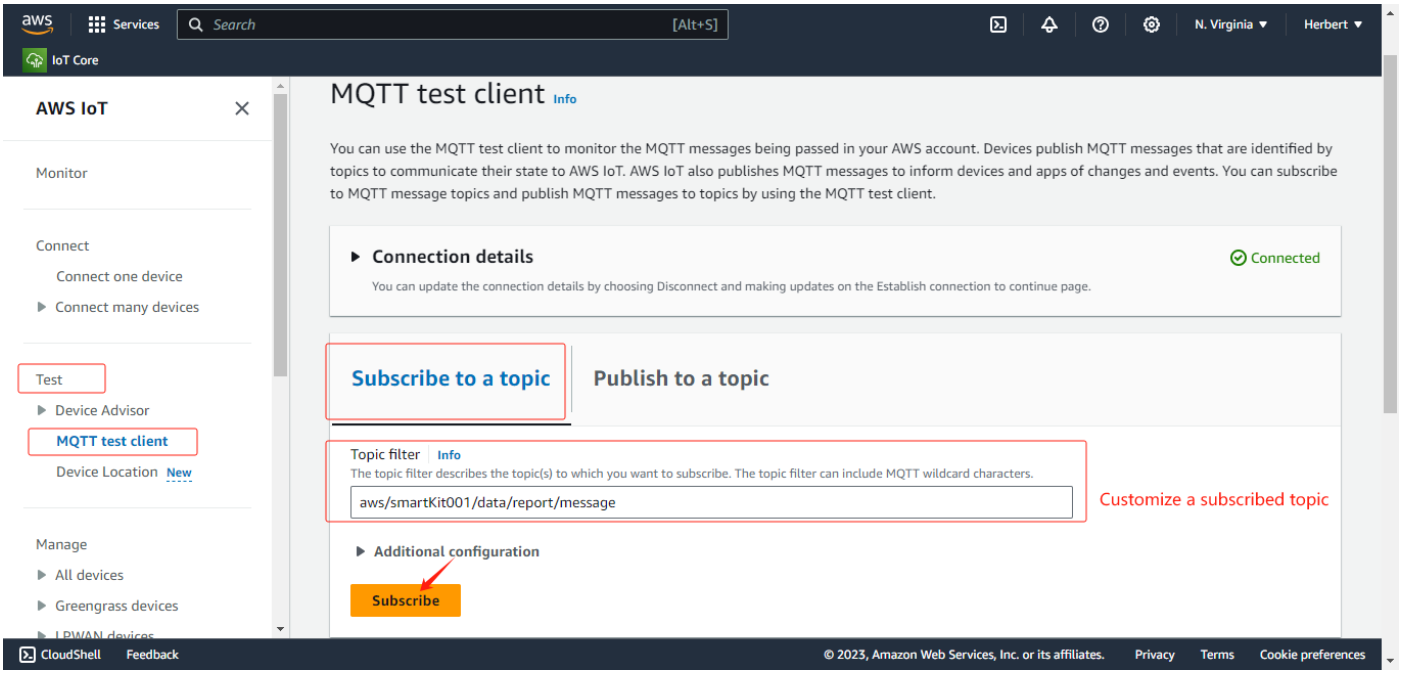


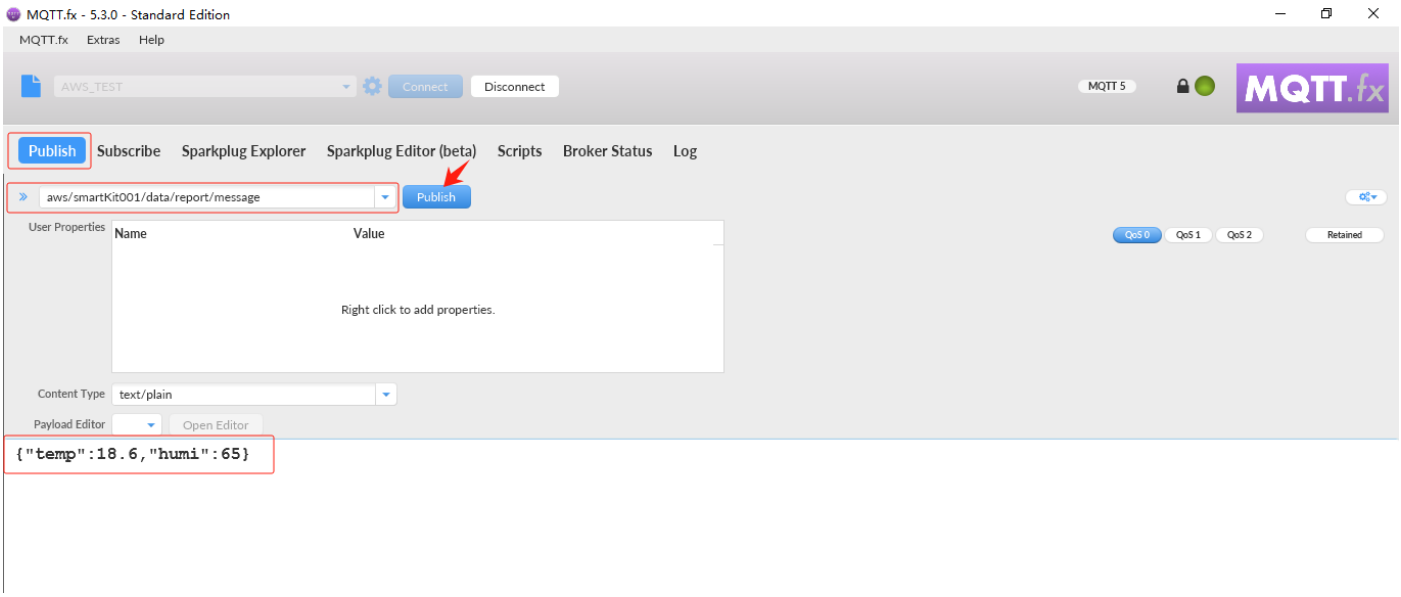


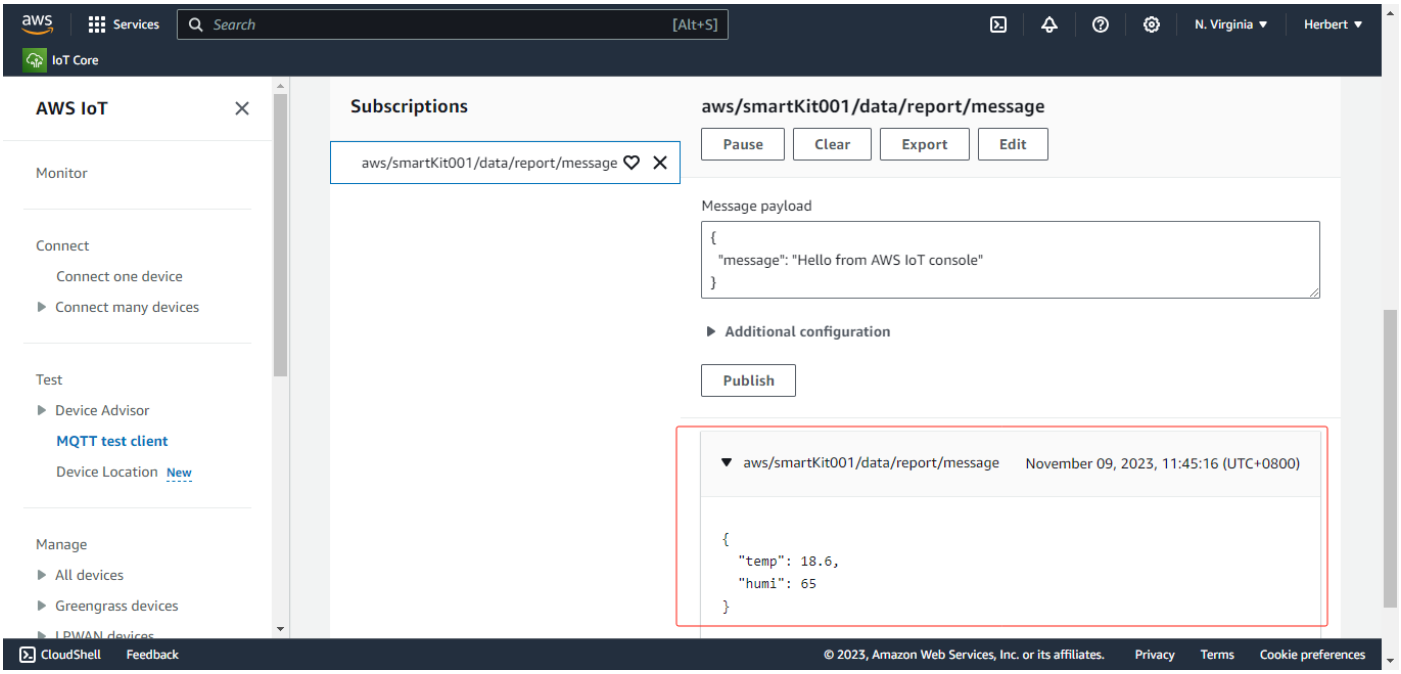


4.2 Client Publish

As shown below, "MQTT test client"based on AWS IoT platform,you can verifie and debug the connected terminal; "MQTT test Client" displays "Connected", customizing the relevant subscribed topic, MQtt.fx virtual terminal can publish messages to the topic, and the platform can view the messages published by the terminal;

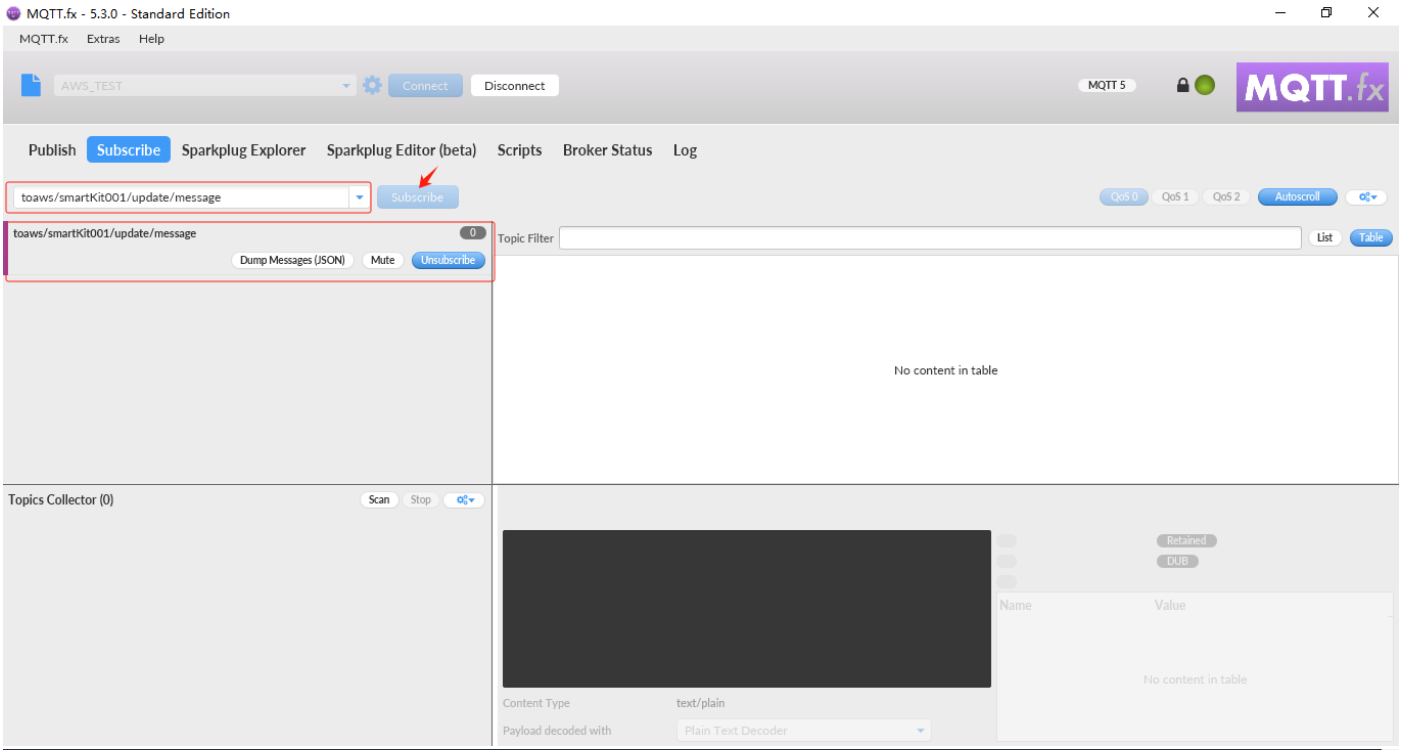


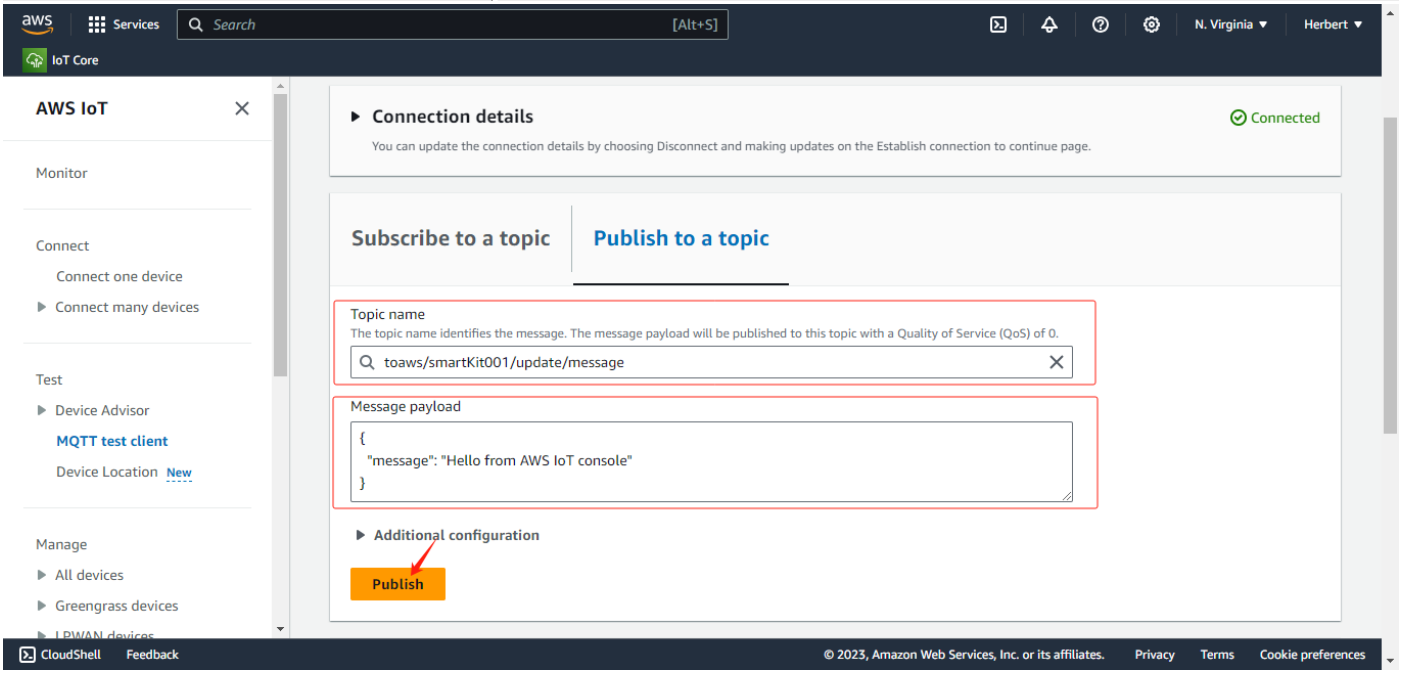


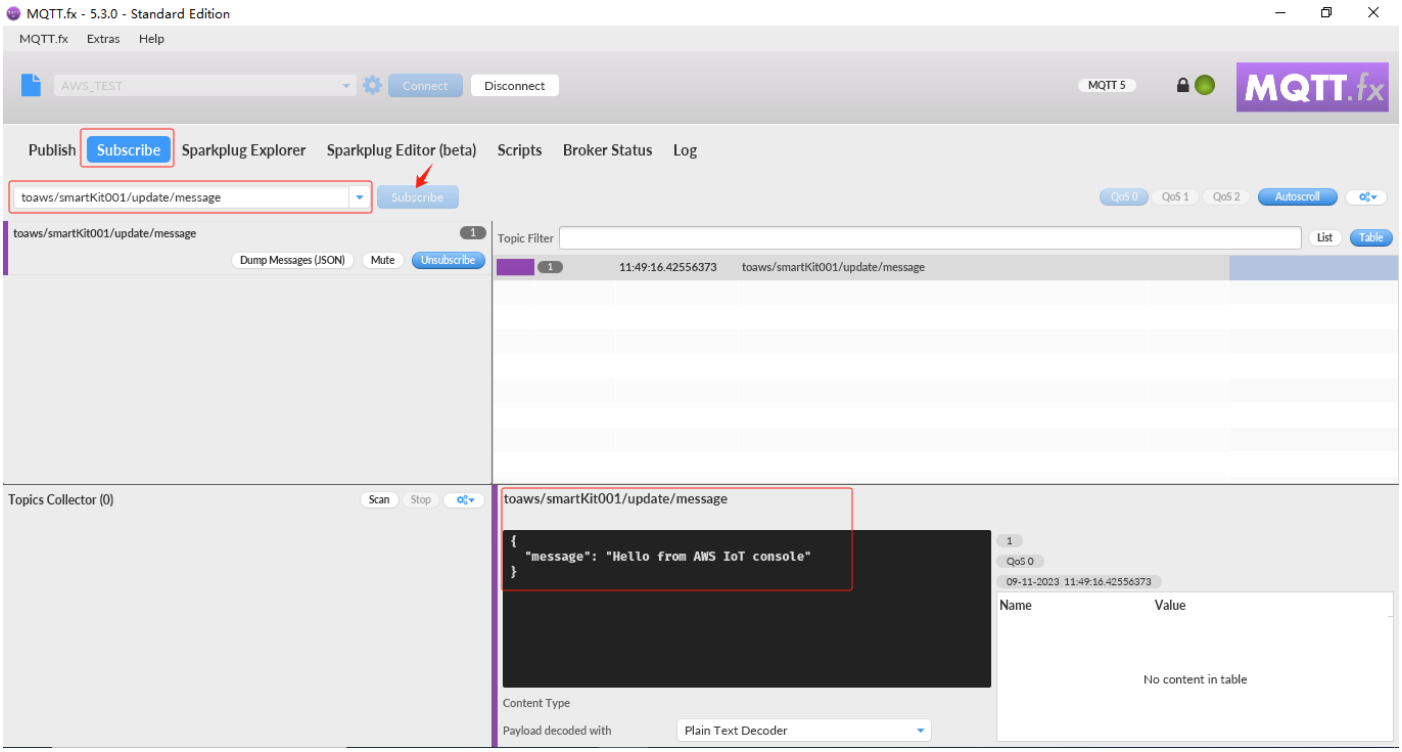


4.3 Client Subscription

As shown below, based on the publication of "MQTT test client" to the Topic, the terminal subscribs to the defined Topic. After the test client clicks "Publish", the MQTT.fx terminal can receive the message of the subscribed Topic.


MQTT.fx - 5.3.0 - Standard Edition
MQTT.fx Extras Help
AWS_TEST
Connect
Disconnect
MQTT 5
MQTT.fx
Publish
Subscribe
Sparkplug Explorer
Sparkplug Editor (beta)
Scripts
Broker Status
Log
toaws/smartKit001/update/message
Subscribe
QoS 0
QoS 1
QoS 2
Autoscroll
toaws/smartKit001/update/message
0
Dump Messages (JSON)
Mute
Unsubscribe
Topic Filter
List
Table
No content in table
Topics Collector (0)
Scan
Stop
Retained
DUB
Name
Value
No content in table
Content Type
text/plain
Payload decoded with
Plain Text Decoder


aws
Services
Search
[Alt+S]
N. Virginia
Herbert
IoT Core
AWS IoT
Monitor
Connect
Connect one device
Connect many devices
Test
Device Advisor
MQTT test client
Device Location New
Manage
All devices
Greengrass devices
LPWAN devices
Connection details
Connected
You can update the connection details by choosing Disconnect and making updates on the Establish connection to continue page.
Subscribe to a topic
Publish to a topic
Topic name
The topic name identifies the message. The message payload will be published to this topic with a Quality of Service (QoS) of 0.
toaws/smartKit001/update/message
Message payload
{
"message": "Hello from AWS IoT console"
}
Additional configuration
Publish
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



五、Module Access to AWS IoT

The following routines for connecting to AWS IoT platform based on Quectel module are as follows:

1) Query the network status of the device and activate the PDP

```
>> AT+CEREG?                                   // Check the network registration status of the terminal
>>
>> +CEREG: 0,1                                 // Network registration succeeded
>>
>> OK
>> AT+QENG="servingcell"                       // Check the network registration status of the terminal
>>
>> +QENG: "servingcell","NOCONN","LTE","FDD",460,11,690843E,314,1850,3,5,5,DF5C,-94,-11,-62,6,34
>>
>> OK
>> AT+QIACT=1                                  // Activate PDP
>>
>> OK
>> AT+CGPADDR=1                                // Query the obtained IP address
>>
>> +CGPADDR: 1,"100.69.28.0,36.14.4.91.4.152.81.115.0.0.0.0.0.0.0.1"
>>
>> OK
```

2) Testing AWS IoT connectivity

```
>> AT+QPING=1,"a9ohm2zbim3d5-ats.iot.us-east-1.amazonaws.com"      // PING the endpoint to verify the connectivity
>>
>> OK
>>
```

```
>> +QPING: 0,"54.172.40.244",32,233,255
>>
>> +QPING: 0,"54.172.40.244",32,234,255
>>
>> +QPING: 0,"54.172.40.244",32,236,255
>>
>> +QPING: 0,"54.172.40.244",32,243,255
>>
>> +QPING: 0,4,4,0,233,243,236
```

3) Load the CA certificate and key files

```
>> AT+QFLST="RAM:*"                          // Check whether a certificate or key file has been stored in RAM
>>
>> OK
>> AT+QFUPL="RAM:cacert.pem",1187,10         // Upload the RootCA.pem to the RAM
>>
>> CONNECT
>> +QFUPL: 1187,2d19                         // The file size must be the same as the certificate size
>>
>> OK
>> AT+QFUPL="RAM:client.pem",1220,10         // Upload the certificate.pem.crt to RAM
>>
>> CONNECT
>> +QFUPL: 1220,2a                           // The file size must be the same as the certificate size
>>
>> OK
>> AT+QFUPL="RAM:user_key.pem",1679,10       // Upload the private.pem.key to RAM
>>
>> CONNECT
>> +QFUPL: 1679,6568                         // The file size must be the same as the certificate size
>>
>> OK
>> AT+QFLST="RAM:*"                          // Check the certificate file and size in RAM
>>
>> +QFLST: "RAM:cacert.pem",1187
>> +QFLST: "RAM:client.pem",1220
>> +QFLST: "RAM:user_key.pem",1679
>>
>> OK
```

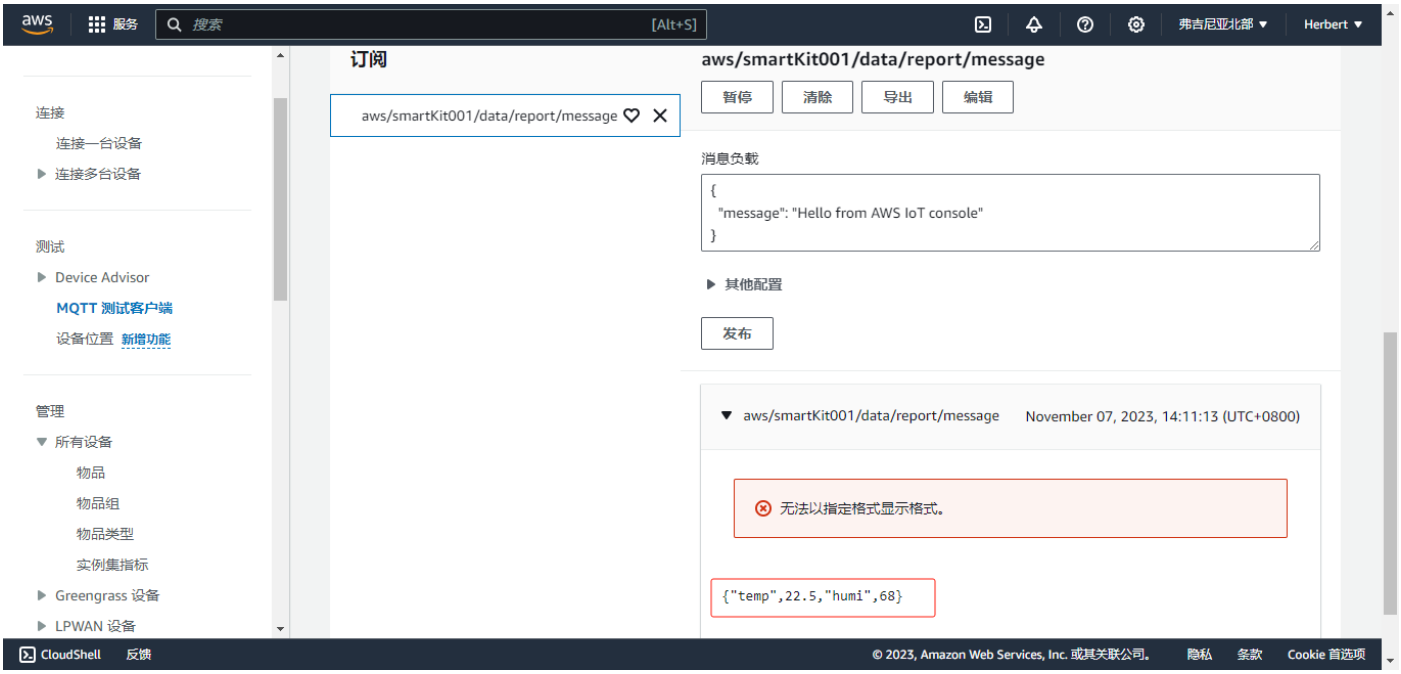
4) MQTT and SSL configuration

```
>> AT+QMTCFG="recv/mode",0,0,1               // Configure receiving mode
>>
>> OK
>> AT+QMTCFG="ssl",0,1,2                     // Configure MQTT connections in SSL mode
>>
>> OK
>> AT+QSSLCFG="cacert",2,"RAM:cacert.pem"    // Configuring the CA Certificate
>>
>> OK
```

```
>> AT+QSSLCFG="clientcert",2,"RAM:client.pem"                    // Configure the clientcert certificate
>>
>> OK
>> AT+QSSLCFG="clientkey",2,"RAM:user_key.pem"                   // Configure the clientkey certificate
>>
>> OK
>> AT+QSSLCFG="seclevel",2,2                                     // SSL authorization mode:server authentication
>>
>> OK
>> AT+QSSLCFG="sslversion",2,4                                   // SSL authorized version
>>
>> OK
>> AT+QSSLCFG="ciphersuite",2,0xFFFF                             // SSL cipher suite
>>
>> OK
>> AT+QSSLCFG="ignorelocaltime",2,1                              // Ignore authorization time
>>
>> OK
```

5) MQTT of AWS IoT connect,subscribe and publish

```
>> AT+QMTOPEN=0,"a9ohm2zbim3d5-ats.iot.us-east-1.amazonaws.com",8883   // Open the MQTT SSL connection
>>
>> OK
>>
>> +QMTOPEN: 0,0
>> AT+QMTCONN=0,"smartKit001"                                    // Initiate the MQTT server connection
>>
>> OK
>>
>> +QMTCONN: 0,0,0
>> AT+QMTSUB=0,1,"toaws/smartKit001/update/message",1            // Subscribe to related topic
>>
>> OK
>>
>> +QMTSUB: 0,1,0,1
>> AT+QMTPUBEX=0,1,1,0,"aws/smartKit001/data/report/message",23  // Publish messages to related topic
>>
>> > {"temp",22.5,"humi",68}
>>
>> OK
>>
>> +QMTPUBEX: 0,1,0
>>
>> +QMTRECV: 0,0,"toaws/smartKit001/update/message",42,"{ "message": "Hello from AWS IoT console"}"
>> AT+QMTCLOSE=0                                                 // Initiating MQTT connection disconnected
>>
>> OK
>>
>> +QMTCLOSE: 0,0
```



六、Troubleshooting Abnormal Issues

If your device fails to connect to the AWS IoT platform, please refer to the following troubleshooting advice:

1) For details, see the procedure and methods in the document.
2) Check whether your device or module is successfully connected to the radio network.
3) Check whether your device or module successfully activates PDP and obtains IP address.
4) Please first verify whether the device data endpoint PING is successful.
5) Check whether the security policy, including TLS version and cipher suite, matches the module configuration parameters.
6) Check whether your CA certificate and key files are completely loaded into FILE.