# Table of Contents

What Is AWS IoT? ................................................................................................................................. 1  
AWS IoT Components ............................................................................................................................... 1  
How to Get Started with AWS IoT ......................................................................................................... 2  
Accessing AWS IoT ................................................................................................................................... 2  
Related Services ...................................................................................................................................... 3  
How AWS IoT Works ................................................................................................................................ 3  

Getting Started with AWS IoT .................................................................................................................. 5  
Sign in to the AWS IoT Console ............................................................................................................ 5  
Register a Device in the Registry .......................................................................................................... 6  
Create and Activate a Device Certificate .................................................................................................. 8  
Create an AWS IoT Policy ....................................................................................................................... 10  
Attach an AWS IoT Policy to a Device Certificate ................................................................................ 12  
Attach a Certificate to a Thing ............................................................................................................... 14  
Configure Your Device ............................................................................................................................ 17  
  Configure an AWS IoT Button ................................................................................................................ 17  
  Configure a Different Device .................................................................................................................. 18  
View Device MQTT Messages with the AWS IoT MQTT Client ................................................................ 18  

Configure and Test Rules ....................................................................................................................... 21  
  Create an SNS Topic .............................................................................................................................. 21  
  Subscribe to an Amazon SNS Topic ...................................................................................................... 23  
  Create a Rule ....................................................................................................................................... 24  
  Test the Amazon SNS Rule ................................................................................................................... 29  
  Next Steps ......................................................................................................................................... 30  

Create and Track an AWS IoT Job ........................................................................................................... 30  
  Connect Your Device to AWS IoT ......................................................................................................... 31  
  Run the Jobs Sample ............................................................................................................................ 31  
  Create a Job Document .......................................................................................................................... 31  
  Create a Job ......................................................................................................................................... 32  
  Execute the Job on a Device .................................................................................................................. 39  
  Tracking Job Progress with Job and Job Execution Events .................................................................... 40  

AWS IoT Button Quickstarts ................................................................................................................... 44  
  AWS IoT Button Wizard Quickstart ...................................................................................................... 44  
  AWS IoT Button AWS CloudFormation Quickstart ............................................................................ 53  
  Next Steps ......................................................................................................................................... 58  

AWS IoT Rule Tutorials ............................................................................................................................ 59  
  Creating a DynamoDB Rule ................................................................................................................... 59  
  Creating a Lambda Rule ....................................................................................................................... 67  
    Create the Lambda Function ................................................................................................................ 67  
    Test Your Lambda Function .............................................................................................................. 73  
  Creating a Lambda Rule .......................................................................................................................... 75  
  Test Your Lambda Rule .......................................................................................................................... 78  
  Creating an Amazon SNS Rule .............................................................................................................. 80  

AWS IoT SDK Tutorials ............................................................................................................................ 88  
  Connecting Your Raspberry Pi .............................................................................................................. 88  
    Prerequisites ...................................................................................................................................... 88  
    Sign in to the AWS IoT Console ......................................................................................................... 88  
    Create and Attach a Thing (Device) ................................................................................................. 90  
  Using the AWS IoT Embedded C SDK ............................................................................................... 97  
    Set Up the Runtime Environment for the AWS IoT Embedded C SDK .............................................. 97  
    Sample App Configuration ............................................................................................................... 97  
    Run Sample Applications ............................................................................................................... 98  
  Using the AWS IoT Device SDK for JavaScript ................................................................................ 99  
    Set Up the Runtime Environment for the AWS IoT Device SDK for JavaScript ............................ 100  
    Install the AWS IoT Device SDK for JavaScript ............................................................................ 101
Topics ........................................................................................................................................... 170
Reserved Topics ....................................................................................................................... 171
Lifecycle Events ....................................................................................................................... 173
   Connect/Disconnect Events .............................................................................................. 174
   Subscribe/Unsubscribe Events ........................................................................................... 174
Rules ........................................................................................................................................ 176
   Granting AWS IoT the Required Access .......................................................................... 176
   Pass Role Permissions ........................................................................................................ 178
   Creating an AWS IoT Rule ................................................................................................. 178
   Viewing Your Rules ........................................................................................................... 182
SQL Versions .......................................................................................................................... 182
   What's New in the 2016-03-23 SQL Rules Engine Version .................................................. 183
Troubleshooting a Rule ........................................................................................................... 184
Rule Error Handling .............................................................................................................. 184
   Error Action Message Format .......................................................................................... 184
   Error Action Example ....................................................................................................... 185
Deleting a Rule ....................................................................................................................... 186
AWS IoT Rule Actions .......................................................................................................... 186
   CloudWatch Alarm Action .............................................................................................. 187
   CloudWatch Metric Action ............................................................................................. 187
   DynamoDB Action ............................................................................................................. 188
   DynamoDBv2 Action ......................................................................................................... 190
   Amazon ES Action ............................................................................................................. 191
   Firehose Action ................................................................................................................. 192
   IoT Analytics Action ......................................................................................................... 192
   Kinesis Action .................................................................................................................... 193
   Lambda Action ................................................................................................................... 194
   Republish Action .............................................................................................................. 195
   S3 Action ............................................................................................................................ 196
   Salesforce Action .............................................................................................................. 197
   SNS Action .......................................................................................................................... 198
   SQS Action .......................................................................................................................... 198
   Step Functions Action ...................................................................................................... 199
AWS IoT SQL Reference .......................................................................................................... 200
   Data Types .......................................................................................................................... 201
   Operators ............................................................................................................................ 204
   Functions ............................................................................................................................. 209
   SELECT Clause ................................................................................................................... 242
   FROM Clause ..................................................................................................................... 244
   WHERE Clause ................................................................................................................... 245
   Literals ................................................................................................................................. 245
   Case Statements ................................................................................................................. 246
   JSON Extensions ................................................................................................................. 246
   Substitution Templates ....................................................................................................... 247
Device Shadow Service ........................................................................................................... 249
   Device Shadow Service Data Flow .................................................................................... 249
   Detecting a Thing Is Connected ........................................................................................ 255
Device Shadow Service Documents .......................................................................................... 256
   Document Properties ......................................................................................................... 257
   Versioning of a Device Shadow ......................................................................................... 257
   Client Token ....................................................................................................................... 258
   Example Document .......................................................................................................... 258
   Empty Sections ................................................................................................................... 258
   Arrays ................................................................................................................................. 259
Using Shadows ........................................................................................................................ 259
   Protocol Support ............................................................................................................... 260
   Updating a Shadow ............................................................................................................ 260
AWS IoT Developer Guide

GetV2LoggingOptions ................................................................. 862
ListActiveViolations ............................................................. 864
ListAttachedPolicies .............................................................. 869
ListAuditFindings ................................................................. 872
ListAuditTasks ..................................................................... 881
ListAuthorizers ................................................................... 885
ListCACertificates ................................................................. 888
ListCertificates ................................................................... 891
ListCertificatesByCA ............................................................. 894
ListIndices ........................................................................... 898
ListJobExecutionsForJob ..................................................... 901
ListJobExecutionsForThing .................................................. 905
ListJobs ................................................................................ 908
ListOTAUpdates ................................................................... 913
ListOutgoingCertificates ...................................................... 916
ListPolicies .......................................................................... 920
ListPolicyPrincipals ............................................................. 923
ListPolicyVersions ............................................................... 926
ListPrincipalPolicies ............................................................ 929
ListPrincipalThings .............................................................. 932
ListRoleAliases ................................................................... 935
ListScheduledAudits ............................................................. 938
ListSecurityProfiles .............................................................. 941
ListSecurityProfilesForTarget ............................................... 944
ListStreams .......................................................................... 947
ListTargetsForPolicy ............................................................. 950
ListTargetsForSecurityProfile ............................................... 953
ListThingGroups .................................................................. 956
ListThingGroupsForThing ...................................................... 960
ListThingPrincipals ............................................................... 963
ListThingRegistrationTaskReports ......................................... 965
ListThingRegistrationTasks .................................................... 968
ListThingTypes ..................................................................... 971
ListThings ............................................................................ 975
ListThingsInThingGroup ....................................................... 978
ListTopicRules ..................................................................... 981
ListV2LoggingLevels ............................................................ 984
ListViolationEvents ............................................................... 987
Publish .................................................................................. 993
RegisterCACertificate .......................................................... 995
RegisterCertificate ............................................................... 999
RegisterThing ...................................................................... 1003
RejectCertificateTransfer ...................................................... 1006
RemoveThingFromThingGroup ............................................... 1009
ReplaceTopicRule .................................................................. 1011
SearchIndex ......................................................................... 1028
SetDefaultAuthorizer ............................................................ 1033
SetDefaultPolicyVersion ...................................................... 1035
SetLoggingOptions ............................................................... 1037
SetV2LoggingLevel ............................................................... 1039
SetV2LoggingOptions ............................................................. 1041
StartNextPendingJobExecution ............................................... 1043
StartOnDemandAuditTask ...................................................... 1047
StartThingRegistrationTask .................................................... 1050
StopThingRegistrationTask ..................................................... 1052
TestAuthorization ................................................................. 1054
TestInvokeAuthorizer ........................................................... 1061
<table>
<thead>
<tr>
<th>Operation</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TransferCertificate</td>
<td>1065</td>
</tr>
<tr>
<td>UpdateAccountAuditConfiguration</td>
<td>1068</td>
</tr>
<tr>
<td>UpdateAuthorizer</td>
<td>1072</td>
</tr>
<tr>
<td>UpdateCACertificate</td>
<td>1075</td>
</tr>
<tr>
<td>UpdateCertificate</td>
<td>1078</td>
</tr>
<tr>
<td>UpdateEventConfigurations</td>
<td>1081</td>
</tr>
<tr>
<td>UpdateIndexingConfiguration</td>
<td>1083</td>
</tr>
<tr>
<td>UpdateJobExecution</td>
<td>1085</td>
</tr>
<tr>
<td>UpdateRoleAlias</td>
<td>1091</td>
</tr>
<tr>
<td>UpdateScheduledAudit</td>
<td>1094</td>
</tr>
<tr>
<td>UpdateSecurityProfile</td>
<td>1098</td>
</tr>
<tr>
<td>UpdateStream</td>
<td>1106</td>
</tr>
<tr>
<td>UpdateThing</td>
<td>1110</td>
</tr>
<tr>
<td>UpdateThingGroup</td>
<td>1114</td>
</tr>
<tr>
<td>UpdateThingGroupsForThing</td>
<td>1117</td>
</tr>
<tr>
<td>UpdateThingShadow</td>
<td>1119</td>
</tr>
<tr>
<td>ValidateSecurityProfileBehaviors</td>
<td>1122</td>
</tr>
</tbody>
</table>
What Is AWS IoT?

AWS IoT provides secure, bi-directional communication between Internet-connected devices such as sensors, actuators, embedded micro-controllers, or smart appliances and the AWS Cloud. This enables you to collect telemetry data from multiple devices, and store and analyze the data. You can also create applications that enable your users to control these devices from their phones or tablets.

AWS IoT Components

AWS IoT consists of the following components:

**Device gateway**

Enabled devices to securely and efficiently communicate with AWS IoT.

**Message broker**

Provides a secure mechanism for devices and AWS IoT applications to publish and receive messages from each other. You can use either the MQTT protocol directly or MQTT over WebSocket to publish and subscribe. You can use the HTTP REST interface to publish.

**Rules engine**

Provides message processing and integration with other AWS services. You can use an SQL-based language to select data from message payloads, and then process and send the data to other services, such as Amazon S3, Amazon DynamoDB, and AWS Lambda. You can also use the message broker to republish messages to other subscribers.

**Security and Identity service**

Provides shared responsibility for security in the AWS Cloud. Your devices must keep their credentials safe in order to securely send data to the message broker. The message broker and rules engine use AWS security features to send data securely to devices or other AWS services.

**Registry**

Organizes the resources associated with each device in the AWS Cloud. You register your devices and associate up to three custom attributes with each one. You can also associate certificates and MQTT client IDs with each device to improve your ability to manage and troubleshoot them.

**Group registry**

Groups allow you to manage several devices at once by categorizing them into groups. Groups can also contain groups—you can build a hierarchy of groups. Any action you perform on a parent group will apply to its child groups, and to all the devices in it and in all of its child groups as well. Permissions given to a group will apply to all devices in the group and in all of its child groups.

**Device shadow**

A JSON document used to store and retrieve current state information for a device.

**Device Shadow service**

Provides persistent representations of your devices in the AWS Cloud. You can publish updated state information to a device's shadow, and your device can synchronize its state when it connects. Your devices can also publish their current state to a shadow for use by applications or other devices.
Device Provisioning service

Allows you to provision devices using a template that describes the resources required for your device: a thing, a certificate, and one or more policies. A thing is an entry in the registry that contains attributes that describe a device. Devices use certificates to authenticate with AWS IoT. Policies determine which operations a device can perform in AWS IoT.

The templates contain variables that are replaced by values in a dictionary (map). You can use the same template to provision multiple devices just by passing in different values for the template variables in the dictionary.

Custom Authentication service

You can define custom authorizers that allow you to manage your own authentication and authorization strategy using a custom authentication service and a Lambda function. Custom authorizers allow AWS IoT to authenticate your devices and authorize operations using bearer token authentication and authorization strategies.

Custom authorizers can implement various authentication strategies (for example, JSON Web Token verification, OAuth provider callout, and so on) and must return policy documents that are used by the device gateway to authorize MQTT operations.

Jobs service

Allows you to define a set of remote operations that are sent to and executed on one or more devices connected to AWS IoT. For example, you can define a job that instructs a set of devices to download and install application or firmware updates, reboot, rotate certificates, or perform remote troubleshooting operations.

To create a job, you specify a description of the remote operations to be performed and a list of targets that should perform them. The targets can be individual devices, groups or both.

For information about AWS IoT limits, see AWS IoT Limits.

How to Get Started with AWS IoT

- To learn more about AWS IoT, see How AWS IoT Works (p. 3).
- To learn how to connect a device to AWS IoT, see Getting Started with AWS IoT (p. 5).

Accessing AWS IoT

AWS IoT provides the following interfaces to create and interact with your devices:

- **AWS Command Line Interface (AWS CLI)**—Run commands for AWS IoT on Windows, macOS, and Linux. These commands allow you to create and manage things, certificates, rules, and policies. To get started, see the AWS Command Line Interface User Guide. For more information about the commands for AWS IoT, see `iot` in the AWS CLI Command Reference.

- **AWS IoT API**—Build your IoT applications using HTTP or HTTPS requests. These API actions allow you to programmatically create and manage things, certificates, rules, and policies. For more information about the API actions for AWS IoT, see Actions in the AWS IoT API Reference.

- **AWS SDKs**—Build your IoT applications using language-specific APIs. These SDKs wrap the HTTP/HTTPS API and allow you to program in any of the supported languages. For more information, see AWS SDKs and Tools.

- **AWS IoT Device SDKs**—Build applications that run on devices that send messages to and receive messages from AWS IoT. For more information see, AWS IoT SDKs.
Related Services

AWS IoT integrates directly with the following AWS services:

- **Amazon Simple Storage Service**—Provides scalable storage in the AWS Cloud. For more information, see Amazon S3.
- **Amazon DynamoDB**—Provides managed NoSQL databases. For more information, see Amazon DynamoDB.
- **Amazon Kinesis**—Enables real-time processing of streaming data at a massive scale. For more information, see Amazon Kinesis.
- **AWS Lambda**—Runs your code on virtual servers from Amazon EC2 in response to events. For more information, see AWS Lambda.
- **Amazon Simple Notification Service**—Sends or receives notifications. For more information, see Amazon SNS.
- **Amazon Simple Queue Service**—Stores data in a queue to be retrieved by applications. For more information, see Amazon SQS.

How AWS IoT Works

AWS IoT enables Internet-connected devices to connect to the AWS Cloud and lets applications in the cloud interact with Internet-connected devices. Common IoT applications either collect and process telemetry from devices or enable users to control a device remotely.

Devices report their state by publishing messages, in JSON format, on MQTT topics. Each MQTT topic has a hierarchical name that identifies the device whose state is being updated. When a message is published on an MQTT topic, the message is sent to the AWS IoT MQTT message broker, which is responsible for sending all messages published on an MQTT topic to all clients subscribed to that topic.

Communication between a device and AWS IoT is protected through the use of X.509 certificates. AWS IoT can generate a certificate for you or you can use your own. In either case, the certificate must be registered and activated with AWS IoT, and then copied onto your device. When your device communicates with AWS IoT, it presents the certificate to AWS IoT as a credential.

We recommend that all devices that connect to AWS IoT have an entry in the registry. The registry stores information about a device and the certificates that are used by the device to secure communication with AWS IoT.

You can create rules that define one or more actions to perform based on the data in a message. For example, you can insert, update, or query a DynamoDB table or invoke a Lambda function. Rules use expressions to filter messages. When a rule matches a message, the rules engine invokes the action using the selected properties. Rules also contain an IAM role that grants AWS IoT permission to the AWS resources used to perform the action.
Each device has a shadow that stores and retrieves state information. Each item in the state information has two entries: the state last reported by the device and the desired state requested by an application. An application can request the current state information for a device. The shadow responds to the request by providing a JSON document with the state information (both reported and desired), metadata, and a version number. An application can control a device by requesting a change in its state. The shadow accepts the state change request, updates its state information, and sends a message to indicate the state information has been updated. The device receives the message, changes its state, and then reports its new state.
Getting Started with AWS IoT

This tutorial shows you how to create resources required to send, receive, and process MQTT messages from devices using AWS IoT.

You need the following to complete this tutorial:

- A computer with Wi-Fi access.
- If you have an AWS IoT button (pictured here), you can use it to complete this tutorial.
- If you do not have a button, you can purchase one here or you can use the MQTT client in the AWS IoT console to emulate a device.

For more information about AWS IoT, see What Is AWS IoT (p. 1).

Sign in to the AWS IoT Console

If you do not have an AWS account, create one.

To create an AWS account:

1. Open the AWS home page and choose Create an AWS Account.
2. Follow the online instructions. Part of the sign-up procedure involves receiving a phone call and entering a PIN using your phone's keypad.
3. Sign in to the AWS Management Console and open the AWS IoT console.
4. On the Welcome page, choose Get started.
Register a Device in the Registry

Devices connected to AWS IoT are represented by things in the registry. The registry allows you to keep a record of all of the devices that are connected to your AWS IoT account.

The fastest way to start using your AWS IoT Button is to download the mobile app for iOS or Android. The mobile app creates the required AWS IoT resources for you, and adds an event source to your button that uses a Lambda blueprint to invoke a new AWS Lambda function of your choice. Blueprints are preconfigured Lambda functions that allow you to quickly connect the click of a button to the functions that fit you best, such as sending automated emails or text messages or deploying other AWS services. You can download the mobile apps from The Apple App Store or Google Play.

If you are unable to use the mobile apps, follow these instructions.

**To register your device in the registry:**

1. On the Welcome to the AWS IoT Console page, in the left navigation pane, choose Manage to expand the choices, and then choose Things.
2. On the page that says You don't have any things yet, choose Register a thing.

3. On the Creating AWS IoT things page, choose Create a single thing.
4. On the Create a thing page, in the Name field, type a name for your device, such as MyIoTButton. Choose Next to add your device to the registry.

Create and Activate a Device Certificate

Communication between your device and AWS IoT is protected through the use of X.509 certificates. AWS IoT can generate a certificate for you or you can use your own X.509 certificate. In this tutorial, AWS IoT generates the X.509 certificate for you. Certificates must be activated prior to use.

1. Choose Create certificate.
2. On the **Certificate created!** page, choose **Download** for the certificate, private key, and the root CA for AWS IoT (the public key need not be downloaded). Save each of them to your computer, and then choose **Activate** to continue.

Be aware that the downloaded filenames may be different than those listed on the **Certificate created!** page. For example:

- 2a540e2346-certificate.pem.crt
- 2a540e2346-private.pem.key
- 2a540e2346-public.pem.key

**Note**
Although it is unlikely, root CA certificates are subject to expiration and/or revocation. If this should occur, you must copy new a root CA certificate onto your device.

3. Choose the back arrow until you have returned to the main **AWS IoT** console screen.
Create an AWS IoT Policy

X.509 certificates are used to authenticate your device with AWS IoT. AWS IoT policies are used to authorize your device to perform AWS IoT operations, such as subscribing or publishing to MQTT topics. Your device will present its certificate when sending messages to AWS IoT. To allow your device to perform AWS IoT operations, you must create an AWS IoT policy and attach it to your device certificate.

To create an AWS IoT policy:

1. In the left navigation pane, choose Secure, and then Policies. On the You don't have a policy yet page, choose Create a policy.

2. On the Create a policy page, in the Name field, type a name for the policy (for example, MyIoTButtonPolicy). In the Action field, type iot:Connect. In the Resource ARN field, type *. Select the Allow checkbox. This allows all clients to connect to AWS IoT.
Create an AWS IoT Policy

Note
You can restrict which clients (devices) are able to connect by specifying a client ARN as the resource. The client ARNs follow this format:

```
```

Select the **Add Statement** button to add another policy statement. In the **Action** field, type `iot:Publish`. In the **Resource ARN** field, type the ARN of the topic to which your device will publish.

Note
The topic ARN follows this format:

```
arn:aws:iot:your-region:your-aws-account:topic/iotbutton/your-button-serial-number
```

For example:

```
arn:aws:iot:us-east-1:123456789012:topic/iotbutton/G030JF055364XVRB
```

You can find the serial number on the bottom of your button.

If you are not using an AWS IoT button, after `topic/` in the ARN, place the topic your device publishes to. For example:

```
arn:aws:iot:us-east-1:123456789012:topic/my/topic/here
```

Finally, select the **Allow** check box. This allows your device to publish messages to the specified topic.

3. After you have entered the information for your policy, choose **Create**.
Attach an AWS IoT Policy to a Device Certificate

Now that you have created a policy, you must attach it to your device certificate. Attaching an AWS IoT policy to a certificate gives the device the permissions specified in the policy.

1. In the left navigation pane, choose Secure, and then Certificates.

For more information, see Managing AWS IoT Policies.
2. In the box for the certificate you created, choose ... to open a drop-down menu, and then choose **Attach policy**.

3. In the **Attach policies to certificate(s)** dialog box, select the check box next to the policy you created in the previous step, and then choose **Attach**.
A device must have a certificate, private key and root CA certificate to authenticate with AWS IoT. We recommend that you also attach the device certificate to the thing that represents your device in AWS IoT. This allows you to create AWS IoT policies that grant permissions based on certificates attached to your things. For more information, see Thing Policy Variables (p. 139)

**To attach a certificate to the thing representing your device in the registry:**

1. In the box for the certificate you created, choose ... to open a drop-down menu, and then choose **Attach thing**.
2. In the Attach things to certificate(s) dialog box, select the check box next to the thing you registered, and then choose Attach.

3. To verify the thing is attached, select the box representing the certificate.
4. On the Details page for the certificate, in the left navigation pane, choose Things.

5. To verify the policy is attached, on the Details page for the certificate, in the left navigation pane, choose Policies.
Configure Your Device

Configuring your device allows it to connect to your Wi-Fi network. Your device must be connected to your Wi-Fi network to install required files and send messages to AWS IoT. All devices must install a device certificate, private key, and root CA certificate in order to communicate with AWS IoT.

Note
Pressing the AWS IoT button for 15 seconds will reset it and you will have to reconfigure your Wi-Fi and device certificate.

Configure an AWS IoT Button

The easiest way to configure your AWS IoT button is to use the AWS IoT button smart phone app. You can download it from the Apple App Store or the Google Play Store. If you are unable to use the smart phone app, follow these directions to configure your button.

Turn on your device

1. Remove the AWS IoT button from its packaging, and then press and hold the button until a blue blinking light appears. (This should take no longer than 15 seconds.)
2. The button acts as a Wi-Fi access point, so when your computer searches for Wi-Fi networks, it will find one called **Button ConfigureMe - XXX** where XXX is a three-character string generated by the button. Use your computer to connect to the button’s Wi-Fi access point.

Note
When the blue light stops blinking, the button ceases presenting itself as a Wi-Fi access point. Therefore, if you can't complete the following procedure soon enough, you may need to invoke the blue blinking light a few times to do so. Once configured, the device does not need to present itself as a Wi-Fi access point and communicates to the internet, just like any other computer, using your local Wi-Fi network.
3. The first time you connect to the button's Wi-Fi access point, you will be prompted for the WPA2-PSK password. Type the last 8 characters of the device serial number (DSN). You’ll find the DSN on the back of the device, as shown here:

   "DSN:XXXX XXXX XXXX XXXX"

   - Model No: JTNBP
   - FCC ID: 2ACBE-0610
   - Assembled in China

Copy your device certificate and private key onto your AWS IoT button

To connect to AWS IoT, you must copy your device certificate and private key onto the AWS IoT button.

1. In a browser, navigate to http://192.168.0.1/index.html.
2. Complete the configuration form:
   - Type your Wi-Fi SSID and password.
   - Browse to and select your certificate and private key. For example, 2a540e2346-certificate.pem.crt and 2a540e2346-private.pem.key, respectively.
   - Find your custom endpoint in the AWS IoT console. (From the dashboard, in the left navigation pane, choose Manage, and then choose Things. Select the box representing your button to show
its details page. On the details page, in the left navigation pane, choose **Interact** and look for the **HTTPS** section, near the top.) Your endpoint will look something like the following:

```
ABCDEFG1234567.iot.us-east-2.amazonaws.com
```

where `ABCDEFG1234567` is the subdomain and `us-east-2` is the region.

- On the **Button ConfigureMe** page, type the subdomain, and then choose the region that matches the region in your AWS IoT endpoint.

- Select the **Terms and Conditions** check box. Your settings should now look like the following:

```
Button ConfigureMe
```

- Choose **Configure**. Your button should now connect to your Wi-Fi network.

### Configure a Different Device

Consult your device’s documentation to connect to it and copy your device certificate, private key, and root CA certificate onto your device.

### View Device MQTT Messages with the AWS IoT MQTT Client

You can use the AWS IoT MQTT client to better understand the MQTT messages sent by a device.

Devices publish MQTT messages on topics. You can use the AWS IoT MQTT client to subscribe to these topics to see these messages.

**To view MQTT messages:**

1. In the **AWS IoT console**, in the left navigation pane, choose **Test**.
2. Subscribe to the topic on which your thing publishes. In the case of the AWS IoT button, you can subscribe to `iotbutton/+` (note that `+` is the wildcard character). In **Subscribe to a topic**, in the **Subscription topic** field, type `iotbutton/+`, and then choose **Subscribe to topic**.

Choosing **Subscribe to topic** above, results in the topic `iotbutton/+` appearing in the **Subscriptions** column.
3. Press your AWS IoT button, and then view the resulting message in the AWS IoT MQTT client. If you do not have a button, you will simulate a button press in the next step.

Note
The AWS IoT Button FAQs contains useful button LED color pattern information.

4. To use the AWS IoT console to publish a message:

On the MQTT client page, in the Publish section, in the Specify a topic and a message to publish... field, type `iotbutton/ABCDEFG12345`. In the message payload section, type the following JSON:

```json
{
   "serialNumber": "ABCDEFG12345",
   "clickType": "SINGLE",
   "batteryVoltage": "2000 mV"
}
```

Choose Publish to topic. You should see the message in the AWS IoT MQTT client (choose iotbutton/+ in the Subscription column to see the message).
Configure and Test Rules

The AWS IoT rules engine listens for incoming MQTT messages that match a rule. When a matching message is received, the rule takes some action with the data in the MQTT message (for example, writing data to an Amazon S3 bucket, invoking a Lambda function, or sending a message to an Amazon SNS topic). In this step, you will create and configure a rule to send the data received from a device to an Amazon SNS topic. Specifically, you will:

- Create an Amazon SNS topic.
- Subscribe to the Amazon SNS topic using a cell phone number.
- Create a rule that will send a message to the Amazon SNS topic when a message is received from your device.
- Test the rule using your AWS IoT button or an MQTT client.

In the upper-right corner of this page, there is a Filter View drop-down list. For instructions for testing your rule by using the AWS IoT button, choose AWS IoT Button. For instructions for testing your rule by using the AWS IoT MQTT client, choose MQTT Client.

Create an SNS Topic

Use the Amazon SNS console to create an Amazon SNS topic.

**Note**
Amazon SNS is not available in all AWS regions.

1. Open the Amazon SNS console.
2. On the left pane, choose Topics.
3. Choose **Create new topic**.

4. Type a topic name and a display name, and then choose **Create topic**.
5. Make a note of the ARN for the topic you just created.

Subscribe to an Amazon SNS Topic

To receive SMS messages on your cell phone, subscribe to the Amazon SNS topic.

1. In the Amazon SNS console, select the check box next to the topic you just created. From the Actions menu, choose Subscribe to topic.

2. On Create subscription, from the Protocol drop-down list, choose SMS.

   In the Endpoint field, type the phone number of an SMS-enabled cell phone, and then choose Create subscription.
Create a Rule

AWS IoT rules consist of a topic filter, a rule action, and, in most cases, an IAM role. Messages published on topics that match the topic filter trigger the rule. The rule action defines which action to take when the rule is triggered. The IAM role contains one or more IAM policies that determine which AWS services the rule can access. You can create multiple rules that listen on a single topic. Likewise, you can create a single rule that is triggered by multiple topics. The AWS IoT rules engine continuously processes messages published on topics that match the topic filters defined in the rules.

In this example, you will create a rule that uses Amazon SNS to send an SMS notification to a cell phone number.

1. In the AWS IoT console, in the left navigation pane, choose Act.

2. On the Act page, choose Create a rule.
3. On the Create a rule page, in the Name field, type a name for your rule. In the Description field, type a description for the rule.

4. Scroll down to Message source. Choose the latest version from the Using SQL version drop-down list. In the Attribute field, type *. This specifies that you want to send the entire MQTT message that triggered the rule.
5. The rules engine uses the topic filter to determine which rules to trigger when an MQTT message is received. In the **Topic filter** field, type `iotbutton/your-button-DSN`. If you are not using an AWS IoT button, type `my/topic` or the topic used in the rule.

   **Note**
   You can find the DSN on the bottom of the button.

   Leave **Condition** blank.

6. In **Set one or more actions**, choose **Add action**.
7. On the **Select an action** page, select **Send a message as an SNS push notification**, and then choose **Configure action**.

8. On the **Configure action** page, from the **SNS target** drop-down list, choose the Amazon SNS topic you created earlier.
9. Now give AWS IoT permission to publish to the Amazon SNS topic on your behalf when the rule is triggered. Choose **Create a new role**. Enter a name for your new role in the **IAM role name** field. After you have entered the name, choose **Create a new role** again. Select the newly created role from the **IAM role name** drop-down list.

10. Choose **Update role** to apply the permissions to the newly created role, and then choose **Add action**.
11. On the **Create a Rule** page, choose **Create rule**.

For more information about creating rules, see [AWS IoT Rules](#).

**Test the Amazon SNS Rule**

You can test your rule by using an AWS IoT button or the AWS IoT MQTT client.

**AWS IoT Button**

Press your button. You should receive an SMS text that shows the current battery charge level on your device (among other things). Try a long press (about 2 seconds) and a fast double pressing, and note the resulting messages.
To test your rule with the AWS IoT MQTT client:

1. In the AWS IoT console, in the left navigation pane, choose Test.
2. On the MQTT client page, in the Publish section, in the Specify a topic and a message to publish… field, type my/topic or the topic you used in the rule. In the message payload section, type the following JSON:

   ```json
   {
     "message": "Hello, from AWS IoT console"
   }
   ```

   **Note**
   If you are using a button, type iobutton/your-button-DSN instead of my/topic in the Specify a topic and a message to publish… field.

3. Choose Publish to topic. You should receive an Amazon SNS message on your cell phone.

Congratulations! You have successfully created and configured a rule that sends data received from a device to an Amazon SNS topic.

**Next Steps**

For more information about AWS IoT rules, see AWS IoT Rule Tutorials (p. 59) and AWS IoT Rules (p. 176).

**Create and Track an AWS IoT Job**

AWS IoT jobs enable you to deploy and track management tasks in your device fleet. You can use jobs to send remote actions to one or many devices at once, control the deployment of jobs to your devices, and track the current and past status of job executions for each device.
This topic shows how to create and deploy a sample job to a device. It walks you through the steps required to create a job and track its events on a device that is configured to communicate with AWS IoT. These instructions assume that you're using a Raspberry Pi, but they could be adapted for other Linux-based devices.

Here are some possible scenarios for using jobs:

- Updating device firmware, software, or files, such as security certificates.
- Performing administrative tasks, such as restarting devices or performing diagnostics.
- Restoring devices to factory settings or other known good states.

## Connect Your Device to AWS IoT

Perform the following steps to connect a Raspberry Pi to AWS IoT.

1. Complete the Connecting Your Raspberry Pi tutorial. When you're done, you'll have an AWS IoT thing registered in your AWS account named `MyRaspberryPi`. You'll also have fully configured security certificates on your device.

2. Complete the Using the AWS IoT Device SDK for JavaScript tutorial. When you're done, your device will be connected to AWS IoT, and you'll be able to run the sample code that comes with the AWS IoT Device SDK for JavaScript.

Now your device is ready to use AWS IoT jobs.

## Run the Jobs Sample

The AWS IoT Device SDK for JavaScript includes a sample named `jobs-example.js`. This sample can receive messages from the AWS IoT console to verify connectivity with the AWS IoT platform. It can also receive and process job executions that originate from the AWS IoT jobs service.

You can run this sample by using the following command. Use the REST endpoint of your Raspberry Pi as the value of the `-H` parameter.

```
node examples/jobs-example.js -f ~/certs -H <PREFIX>.iot.<REGION>.amazonaws.com -T thingName
```

If you've created a configuration file that contains the thing name and the host endpoint (the REST endpoint of your device), you can use the following command.

```
node examples/jobs-example.js -f ./certs -F your config file name.json
```

## Create a Job Document

A job document is a JSON document that provides all of the information that your device needs to execute a job. The AWS IoT Device SDK for JavaScript uses a property named `operation` to route job documents to specific handlers. The `jobs-example.js` program has a sample handler for an operation named `customJob`. We're going to create a job document named `example-job.json` for this handler. The `example-job.json` file should contain the following JSON object.
Create a Job

Now you're ready to create a job that delivers the job document to all of the devices that you specify. To create a job, you can use the AWS IoT console, the AWS IoT SDK, or the AWS IoT CLI.

The following example shows how to create a job by using the AWS IoT CLI.

```bash
aws iot create-job \
  --job-id "example-job-01" \
  --targets "arn:aws:iot:::thing/MyRaspberryPi" \
  --document file:///example-job.json \
  --description "My First test job" \
  --target-selection SNAPSHOT
```

If you store your job document in Amazon Simple Storage Service, use the `--document-source` parameter instead of the `--document` parameter to specify the Amazon S3 URL for the job document.

If you prefer to use the AWS IoT console, follow these steps to create a job:

1. Upload the job document to an Amazon S3 bucket. For information about uploading documents to Amazon S3, see How Do I Upload Files and Folders to an S3 Bucket? in the Amazon Simple Storage Service Console User Guide.
2. In the AWS IoT console, choose Manage, and then choose Jobs.
3. Choose Create a job.
4. On the Select a job page, choose Create custom job.
AWS IoT Developer Guide
Create a Job

CREATE JOB

Select a job

AWS IoT Device Management job orchestration and notification is a set of remote operations called jobs that are sent to and executed on devices connected to AWS IoT.

Create a custom job
Send a request to acquire an executable job file from one of your devices connected to AWS IoT.

Create an Amazon FreeRTOS Over-the-air (OTA) update job
This OTA update job will send your firmware image securely over the network to FreeRTOS-based devices.

Create a Greengrass Core update job
Create a snapshot job to update one or more Greengrass Core devices with a new Greengrass Core or OTA agent version.
5. On the Create a job page, enter a unique job ID. Under Select devices to update, select the device that you connected to AWS IoT.
Create a job

Job ID

example-job-01

Description

Select devices to update

Browse and select the devices you want to include in this job.

1 thing(s) and 0 thing group(s) selected.

<table>
<thead>
<tr>
<th>Things</th>
<th>Thing Groups</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyRaspberryPi</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
6. Scroll down to **Add a job file** and choose the job document file that you uploaded to Amazon S3. Under **Job type**, select **Your job will complete after deploying to the selected devices/groups (snapshot)**. (The other option, **Your job will continue deploying to any devices added to the selected groups (continuous)**, is for deploying a job to groups of devices as devices are added to each group.) Leave the **Job executions rollout configuration** unchanged. Choose **Create**.
Add a job file

Upload a job file that defines what your job should do.

example-job.json

Pre-sign resource URLs

For an extra layer of security, you can pre-sign URLs that refer to resources in the role associated with the job. You can use the pre-sign URL placeholder in the job file to reference resources.

Cannot find pre-sign url placeholder in the job file. Skip pre-sign configuration.

Job type

A job can run on the devices and/or groups selected, or remain open to deploy to new devices.

Your job will complete after deploying to the selected devices

Your job will continue deploying to any devices added to the list

Job executions rollout configuration

Specify how quickly devices will be notified of a pending job execution.

Maximum per minute (1-1000)

1000
7. Your new job appears on the **Jobs** page.

For more information about creating and deploying jobs, see the [AWS IoT Jobs documentation](#).

**Execute the Job on a Device**

After your job is created, the jobs service sends a notification of a pending job to your device. Your device gets the job details and job document through the `NextJobExecutionChanged` API. The `jobs-example.js` sample that you've already run executes the job on the device. When the job is complete, the sample publishes its completed status by using the `UpdateJobExecution` API. When you run the sample on your device, you'll see the following output.

```bash
node examples/jobs-example.js -f ./certs -F config.json
connect
startJobNotifications completed for thing: MyRaspberryPi
customJob operation handler invoked, jobId: example-job-01
```

When you refresh the **Jobs** page, you can see that your job has successfully completed.
Tracking Job Progress with Job and Job Execution Events

You can use Job events and JobExecution events to track the progress of your job.

This is a helpful way to alert users, system administrators, or other members of your system that a job is complete or that a job execution has changed its status. For example, you can alert a user about a firmware update on a device or inform a system administrator about an issue in their device fleet that needs to be investigated and resolved.

Job events for the job in this example are published to the following topics when the job is completed or canceled.

```
/aws/events/job/example-job-01/completed
/aws/events/job/example-job-01/canceled
```

Job execution events for the job in this example are sent to the following topics when the job execution reaches one of the possible final statuses.

```
/aws/events/jobExecution/example-job-01/succeeded
/aws/events/jobExecution/example-job-01/failed
/aws/events/jobExecution/example-job-01/rejected
/aws/events/jobExecution/example-job-01/canceled
/aws/events/jobExecution/example-job-01/removed
```
When the job execution on your device succeeds, AWS IoT publishes a `JobExecutionsucceeded` event. You can see this event by navigating to the AWS IoT Test page and subscribing to the `$aws/events/jobExecution/example-job-01/succeeded` topic in the MQTT client.

The following message appears when the job execution for your device has successfully completed.
AWS IoT also publishes a completed job event. You can see this event by subscribing to the $aws/events/job/example-job-01/completed topic in the MQTT client.
Publish

Specify a topic and a message to publish with a QoS of 0.

```
$aws/events/job/example-job-01/completed
```

```
1 {
2   "message": "Hello from AWS IoT console"
3 }
```

```
{
   "eventType": "JOB",
   "eventId": "a1817d74-0f1d-42b3-b03f-accfc90af41e",
   "timestamp": "1513709645",
   "operation": "completed",
   "jobId": "example-job-01",
   "status": "COMPLETED",
   "targetSelection": "SNAPSHOT",
   "targets": [
   ],
   "description": "Job example-job-01 for Thing MyRaspberry completedAt": "1513709645105",
   "createdAt": "1513709615488",
   "lastUpdatedAt": "1513709645105",
   "jobProgressDetails": {
      "numberOfCanceledThings": 0,
      "numberOfRejectedThings": 0,
      "numberOfFailedThings": 0,
      "numberOfRemovedThings": 0,
      "numberOfSucceededThings": 1
   }
}```
AWS IoT Button Quickstarts

The two quickstarts in this section show you how to configure and use the AWS IoT button. You can use the AWS IoT button wizard in the AWS Lambda console to easily and quickly configure your AWS IoT button. The AWS Lambda console contains a blueprint that automates the process of setting up your AWS IoT button by:

- Creating and activating an X.509 certificate and private key for authenticating with AWS IoT.
- Walking you through the configuration of your AWS IoT button in order to connect to your Wi-Fi network.
- Walking you through the copying of your certificate and private key to your AWS IoT button.
- Creating and attaching to the certificate an AWS IoT policy that gives the button permission to make calls to AWS IoT.
- Creating an AWS IoT rule that invokes a Lambda function when your AWS IoT button is pressed.
- Creating an IAM role and policy that allows the Lambda function to send email messages using Amazon SNS.
- Creating a Lambda function that sends an email message to the address specified in the Lambda function code.

The second quickstart shows you how to use an AWS CloudFormation template to configure the AWS IoT resources required to process the MQTT messages that are sent when the AWS IoT button is pressed.

If you do not have a button, you can purchase one here. For more information about AWS IoT, see What Is AWS IoT (p. 1).

Topics
- AWS IoT Button Wizard Quickstart (p. 44)
- AWS IoT Button AWS CloudFormation Quickstart (p. 53)
- Next Steps (p. 58)

AWS IoT Button Wizard Quickstart

The AWS IoT button wizard is a Lambda blueprint, so you must sign in to the AWS Lambda console in order to use it. If you do not have an AWS account, you can create one by following these steps.

To create an AWS account

1. Open the AWS home page and choose Create an AWS Account.
2. Follow the online instructions. Part of the sign-up procedure involves receiving a phone call and entering a PIN using your phone's keypad.

To configure the AWS IoT Button

1. Sign in to the AWS Management Console and open the AWS Lambda console.
2. If this is your first time in the AWS Lambda console, you see the following page. Choose the Get Started Now button.

3. On the Select blueprint page, from the Runtime drop-down menu, choose Node.js 4.3. In the filter text box, type button. To choose the iot-button-email blueprint, double-click it or choose the Next button.
4. On the **Configure triggers** page, from the **IoT Type** drop-down menu, choose **IoT Button**.

Type the serial number for your device. The device serial number (DSN) appears on the back of the button.

Choose **Generate certificate and keys**.

**Note**
You only need to generate a certificate and private key once. Then you can navigate to http://192.168.0.1/index.html in a browser to configure your button.
Use the links on the page to download the device certificate and the private key.
The page also includes instructions for configuring your AWS IoT button. On step 3, you choose a link to open a web page that allows you to connect the AWS IoT button to your network. Under **WiFi Configuration**, type the network ID (SSID) and network password for your Wi-Fi network. Under **AWS IoT Configuration**, choose the certificate and private key you downloaded earlier. This copies your certificate and private key to your AWS IoT button. Select the check box to agree to the AWS IoT button terms and conditions, and then choose the **Configure** button.
Button ConfigureMe

Enter the value for any field that you wish to change for device:

Wi-Fi Configuration:
SSID
Guest
Security
☑ Open Network (No Password)
Password
None (unsecured)

AWS IoT Configuration:
Certificate
Browse...
certificate.pem
Private Key
Browse...
private.key
Endpoint Subdomain
AST2RR8XSNT910
Endpoint Region
us-west-2
Final Endpoint
.iot.us-west-2.amazonaws.com

☑ By clicking this box, you agree to the AWS IoT Button Terms and Conditions.

Configure

A configuration confirmation page is displayed.

Button ConfigureMe Setup

Thank you for configuring your device.

If you are unable to use your device, please enter configuration mode and try again.

5. Close the Configure tab and go back to the AWS Lambda console page. Choose Enable trigger, and then choose Next.

On the Configure function page, type a name for your function. The description, runtime, and Lambda function code is entered for you.
In the Lambda function code, replace the example email address with your own email address.
In the Lambda function handler and role section, from the Role drop-down menu, choose Create new role from template(s). Type a unique name for the role.

At the bottom of the page, choose Next.

Review the settings for the Lambda function, and then choose Create function.
You should see a page that confirms your Lambda function has been created:
To test your Lambda function, choose the **Test** button. After about a minute, you should receive an email message with **AWS Notification - Subscription Confirmation** in the subject line. Choose the link in the email message to confirm the subscription to an SNS topic created by the Lambda function. When AWS IoT receives a message from your button, it sends a message to Amazon SNS. The Lambda function created a subscription to the Amazon SNS topic using the email address you added in the code. When Amazon SNS receives a message on this Amazon SNS topic, it forwards the message to your subscribed email address.

Press your button to send a message to AWS IoT. The message causes your Lambda rule to be triggered, and then your Lambda function is invoked. The Lambda function checks if your SNS topic exists. The Lambda function then sends the contents of the message to the Amazon SNS topic. Amazon SNS then forwards the message to the email address you specified in the Lambda function code.

---

**AWS IoT Button AWS CloudFormation Quickstart**

When the AWS IoT button is pressed, it sends basic information about the button to an Amazon SNS topic. The topic then forwards that information to you in an email message. This quickstart shows you how to use an AWS CloudFormation template to configure your AWS IoT button.

You need an AWS account and an AWS IoT button to complete the steps in this quickstart.

1. Use the AWS IoT console to create an AWS IoT certificate:
   a. Open the **AWS IoT console**.
   b. If a **Welcome** page appears, choose **Get started**.
c. In the AWS region selector, choose the AWS region where you want to create the AWS IoT certificate (for example, US East (N. Virginia)). You will be creating all supporting AWS resources (additional AWS IoT resources and an Amazon SNS resource) in the same AWS region.
d. On the Dashboard, in the left navigation pane, choose Security, and then choose Certificates.
e. On the Certificates pane, choose Create.
f. Choose One-click certificate creation - Create certificate.
g. On the Certificate created page, choose Download for the certificate, private key, and root CA for AWS IoT, save each of them to your computer, and then choose Activate.
h. Choose Done.
i. On the Certificates page, choose the certificate you just created.
j. In the Details pane, make a note of the certificate ARN value (for example, arn:aws:iot:region-ID:account-ID:cert/random-ID). You need it later in this procedure.

2. Use the AWS CloudFormation console at https://console.aws.amazon.com/cloudformation/ to create the AWS IoT resources, an Amazon SNS resource, and an IAM role:
a. Save the following AWS CloudFormation template file named AWSIoTButtonQuickStart.template to your computer.

   **Note**
   Check the DSN for your button. Make sure the beginning of the "AllowedPattern" string matches your DSN.

```json
{
"AWSTemplateFormatVersion": "2010-09-09",
"Description": "Creates required AWS resources to allow an AWS IoT button to send information through an Amazon Simple Notification Service (Amazon SNS) topic to an email address.",
"Parameters": {
  "IoTButtonDSN": {
    "Type": "String",
    "Description": "The device serial number (DSN) of the AWS IoT Button. This can be found on the back of the button. The DSN must match the pattern of 'G030[A-Z][0-9][0-9][0-9][0-9][0-5][1-7][0-9A-HJ-NP-X][0-9A-HJ-NP-X][0-9A-HJ-NP-X][0-9A-HJ-NP-X][0-9A-HJ-NP-X]'"},
  "CertificateARN": {
    "Type": "String",
    "Description": "The Amazon Resource Name (ARN) of the existing AWS IoT certificate."
  },
  "SNSTopicName": {
    "Type": "String",
    "Default": "aws-iot-button-sns-topic",
    "Description": "The name of the Amazon SNS topic for AWS CloudFormation to create."
  },
  "SNSTopicRoleName": {
    "Type": "String",
    "Default": "aws-iot-button-sns-topic-role",
    "Description": "The name of the IAM role for AWS CloudFormation to create. This IAM role allows AWS IoT to send notifications to the Amazon SNS topic."
  },
  "EmailAddress": {
    "Type": "String",
    "Description": "The email address for the Amazon SNS topic to send information to."
  }
}
```
"Resources": {
    "IoTThing": {
        "Type": "AWS::IoT::Thing",
        "Properties": {
            "ThingName": {
                "Fn::Join": [ "", [
                    "iotbutton_",
                    { "Ref": "IoTButtonDSN" }
                ]
            }
        }
    },
    "IoTPolicy": {
        "Type": "AWS::IoT::Policy",
        "Properties": {
            "PolicyDocument": {
                "Version": "2012-10-17",
                "Statement": [
                    {
                        "Action": "iot:Publish",
                        "Effect": "Allow",
                        "Resource": {
                            "Fn::Join": [ "", [
                                "arn:aws:iot:",
                                { "Ref": "AWS::Region" },
                                ":",
                                { "Ref": "AWS::AccountId" },
                                ":topic/iotbutton/",
                                { "Ref": "IoTButtonDSN" }
                            ]
                        }
                    }
                ]
            }
        }
    },
    "IoTPolicyPrincipalAttachment": {
        "Type": "AWS::IoT::PolicyPrincipalAttachment",
        "Properties": {
            "PolicyName": { "Ref": "IoTPolicy" },
            "Principal": { "Ref": "CertificateARN" }
        }
    },
    "IoTThingPrincipalAttachment": {
        "Type": "AWS::IoT::ThingPrincipalAttachment",
        "Properties": {
            "Principal": { "Ref": "CertificateARN" }
        }
    },
    "SNSTopic": {
        "Type": "AWS::SNS::Topic",
        "Properties": {
            "TopicName": { "Ref": "SNSTopicName" }
        }
    }
},
"SNSTopic": {
    "Type": "AWS::SNS::Topic",
    "Properties": {
        "TopicName": { "Ref": "SNSTopicName" }
    }
}
"DisplayName": "AWS IoT Button Press Notification",
"Subscription": [
  {
    "Endpoint": {
      "Ref": "EmailAddress"
    },
    "Protocol": "email"
  },
  "TopicName": {
    "Ref": "SNSTopicName"
  }
],
"SNSTopicRole": {
  "Type": "AWS::IAM::Role",
  "Properties": {
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "Service": "iot.amazonaws.com"
          },
          "Action": "sts:AssumeRole"
        }
      ],
      "Path": "/",
      "Policies": [
        {
          "PolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
              {
                "Effect": "Allow",
                "Action": "sns:Publish",
                "Resource": {
                  "Fn::Join": [ "",
                    [ "arn:aws:sns:",
                      { "Ref": "AWS::Region" },
                      ":",
                      { "Ref": "AWS::AccountId" },
                      ":",
                      { "Ref": "SNSTopicName" }
                    ]
                }
              }
            ],
            "PolicyName": {
              "Ref": "SNSTopicRoleName"
            }
          }
        }
      ]
    }
  }
},
"IoTTopicRule": {
  "Type": "AWS::IoT::TopicRule",
  "Properties": {
    "RuleName": {
      "Fn::Join": [ "",
        [ ""]
    }
  }
}

c. Make sure the region where you created the AWS IoT certificate (for example, US East (N. Virginia)) is displayed on the AWS region selector.

d. Choose Create Stack.

e. On the Select Template page, choose Upload a template to Amazon S3, and then choose Browse.

f. Select the AWSIoTButtonQuickStart.template file you saved earlier, choose Open, and then choose Next.

g. On the Specify Details page, for Stack name, type a name for this AWS CloudFormation stack (for example, MyAWSIoTButtonStack).

h. For CertificateARN, type the Amazon Resource Name (ARN) of the AWS IoT certificate (the certificate ARN value) that you noted earlier.

i. For EmailAddress, type your email address.

j. For IoTButtonDSN, type the device serial number (DSN). It appears on the back of your AWS IoT button (for example, G030JF051234A5BC).

k. You can leave SNSTopicName and SNSTopicRoleName at their defaults, or specify a different Amazon SNS topic name and associated IAM role name. For example, if you plan to set up more AWS IoT buttons, you might want to change these values. Choose Next.

l. You do not need to do anything on the Options page. Choose Next.

m. On the Review page, select I acknowledge that AWS CloudFormation might create IAM resources, and then choose Create.
n. When CREATE_COMPLETE is displayed for MyAWSIoTButtonStack, check your email inbox for a message with a subject line of AWS IoT Button Press Notification. Choose the Confirm subscription link in the body of the email message.

3. Using the private key and certificate you created earlier, follow the steps in Configure Your Device to set up your AWS IoT button.

4. After you have set it up, press the button once. A white light should blink several times and then be followed by a steady green light for a few moments. Shortly afterward, you should receive an email message with AWS IoT Button Press Notification in the subject line. It contains information sent by the button in the body of the email message.

5. After you are finished experimenting, you can clean up the AWS resources created by the AWS CloudFormation template. To do this, return to the AWS CloudFormation console and delete MyAWSIoTButtonStack. After you delete MyAWSIoTButtonStack, delete the AWS IoT certificate as follows:
   a. Return to the AWS IoT console.
   b. In the list of resources, select the check box inside of the box that represents the AWS IoT certificate (the box with the handshake icon).
   c. For Actions, choose Deactivate, and then confirm.
   d. With the box that represents the AWS IoT certificate still selected, for Actions, choose Delete, and then confirm.
   e. The private key and certificate that you downloaded earlier are no longer valid, so you can now delete them from your computer.

Next Steps

To learn more about the Lambda blueprint used to set up your button, see Getting Started with AWS IoT. To learn how to use AWS CloudFormation with the AWS IoT button, see http://docs.aws.amazon.com/iot/latest/developerguide/iot-button-cloud-formation.html.
AWS IoT Rule Tutorials

This guide includes tutorials that walk you through the creation and testing of AWS IoT rules. If you have not completed the AWS IoT Getting Started Tutorial (p. 5), we recommend you do that first. It shows you how to create an AWS account and connect your device to AWS IoT.

An AWS IoT rule consists of a SQL SELECT statement, a topic filter, and a rule action. Devices send information to AWS IoT by publishing messages to MQTT topics. The SQL SELECT statement allows you to extract data from an incoming MQTT message. The topic filter of an AWS IoT rule specifies one or more MQTT topics. The rule is triggered when an MQTT message is received on a topic that matches the topic filter. Rule actions allow you to take the information extracted from an MQTT message and send it to another AWS service. Rule actions are defined for AWS services like Amazon DynamoDB, AWS Lambda, Amazon SNS, and Amazon S3. By using a Lambda rule, you can call other AWS or third-party web services. For a complete list of rule actions, see AWS IoT Rule Actions (p. 186).

In these tutorials we assume you are using the AWS IoT button and will use iotbutton/+ as the topic filter in the rules. If you do not have an AWS IoT button, you can buy one here.

Alternatively, you can emulate the AWS IoT button by using an MQTT client like the AWS IoT MQTT client in the AWS IoT console. To emulate the AWS IoT button, publish a similar message on the iotbutton/ABCDEFG12345 topic. The number after the / is arbitrary. It is used as the serial number for the button.

You can also use your own device, but you must know on which MQTT topic your device publishes so you can specify it as the topic filter in the rule. For more information, see AWS IoT Rules (p. 176).

The AWS IoT button sends a JSON payload that looks like this:

```json
{
    "serialNumber" : "ABCDEFG12345",
    "batteryVoltage" : "2000mV",
    "clickType" : "SINGLE"
}
```

Creating a DynamoDB Rule

DynamoDB rules allow you to take information from an incoming MQTT message and write it to a DynamoDB table.

To create a DynamoDB rule:

1. In the AWS IoT console, in the left navigation pane, choose Act.
2. On the **Rules** page, choose **Create**.

3. On the **Create a rule** page, in the **Name** field, type a name for your rule. In the **Description** field, type a description for the rule.
4. Scroll down to **Message source**. Choose the latest version from the **Using SQL version** drop-down list. In the **Attribute** field, type `*`. This specifies that you want to send the entire MQTT message that triggered the rule.

![Image of Message source](image)

4. Scroll down to **Message source**. Choose the latest version from the **Using SQL version** drop-down list. In the **Attribute** field, type `*`. This specifies that you want to send the entire MQTT message that triggered the rule.

5. The rules engine uses the topic filter to determine which rules to trigger when an MQTT message is received. In the **Topic filter** field, type `iotbutton/your-button-DSN`. If you are not using an AWS IoT button, type `my/topic` or the topic used in the rule.

   **Note**
   You can find the DSN on the bottom of the button.

   Leave **Condition** blank.

   ![Image of Topic filter](image)

6. In **Set one or more actions**, choose **Add action**.
7. On the Select an action page, select Insert a message into a DynamoDB table, and then choose Configure action.

8. On the Configure action page, choose Create a new resource.
9. On the Amazon DynamoDB page, choose Create table.

10. On the Create DynamoDB table page, type a name in the Table name field. In Partition key, type SerialNumber. Select the Add sort key check box, and then type ClickType in the Sort key field. Select String for both the partition and sort keys.
11. Choose **Create**. It takes a few seconds to create your DynamoDB table. Close the browser tab where the Amazon DynamoDB console is open. If you do not close the tab, your DynamoDB table will not be displayed in the **Table name** drop-down list on the AWS IoT **Configure action** page.

12. On the **Configure action** page, choose your new table from the **Table name** drop-down list. In **Hash key value**, type `#{serialNumber}`. This instructs the rule to take the value of the `serialNumber` attribute from the MQTT message and write it into the `SerialNumber` column in the DynamoDB table. In **Range key value**, type `#{clickType}`. This writes the value of the `clickType` attribute into the `ClickType` column. Leave **Write message data to this column** blank. By default, the entire message is written to a column in the table named Payload. Choose **Create a new role**.
13. Type a unique name in IAM role name, and then choose the Create a new role button again. Choose the role you just created, choose Update role, and then choose Add action.

14. Choose Create rule to create the rule.
15. A confirmation message shows the rule has been created. Choose the left arrow to return to the Rules page.

16. Test the rule by pressing your configured AWS IoT button or by using an MQTT client to publish a message on a topic that matches your rule's topic filter. Finally, return to the DynamoDB console and select the table you created to view the entry for your button press or message.
Creating a Lambda Rule

You can define a rule that calls a Lambda function, passing in data from the MQTT message that triggered the rule. This allows you to process the incoming message and then call another AWS or third-party service.

In this tutorial, we assume you have completed the AWS IoT Getting Started Tutorial (p. 5) in which you create and subscribe to an Amazon SNS topic using your cell phone number. You will create a Lambda function that publishes a message to the Amazon SNS topic you created in the AWS IoT Getting Started Tutorial (p. 5). You will also create a Lambda rule that calls the Lambda function, passing in some data from the MQTT message that triggered the rule.

In this tutorial, we also assume you are using an AWS IoT button to trigger the Lambda rule. If you do not have an AWS IoT button, you can buy one here or you can use an MQTT client to send an MQTT message that triggers the rule.

Create the Lambda Function

To create the Lambda function:

1. In the AWS Lambda console, choose Get Started Now or, if you have created a Lambda function before, choose Create a Lambda function.
2. On the Blueprints page, in the Add filter field, enter hello-world, and then choose the hello-world blueprint. Choose the Configure button.

3. On the following page, enter a name for your function. Under Role, choose Create a custom role.

   The IAM console opens, allowing you to create an IAM role that Lambda can assume when executing the Lambda function.

   To edit the role's policy to give it permission to publish to your Amazon SNS topic:

   b. Choose Edit to edit the role's policy.
c. Replace the policy document with the following:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "logs:CreateLogGroup",
            "logs:CreateLogStream",
            "logs:PutLogEvents"
         ],
         "Resource": "arn:aws:logs:*:*:*"
      },
      {
         "Effect": "Allow",
         "Action": [
            "sns:Publish"
         ],
         "Resource": "arn:aws:sns:us-east-1:123456789012:MyIoTButtonSNSTopic"
      }
   ]
}
```

This policy document adds permission to publish to your Amazon SNS topic.

**Note**
Replace the value of the second Resource with the ARN of the Amazon SNS topic you created previously.

4. Choose **Allow**. The IAM console closes.
5. Return to the Lambda console. Choose **Create function**.
6. On the function **Configuration** page, select **AWS IoT** from the column on the left. A **Configure triggers** section will appear on the page.

7. In the **Device Serial Number** field, type your button's device serial number (DSN). The DSN is printed on the back of your AWS IoT button. If you have not already generated a certificate and private key for your AWS IoT button, choose **Generate certificate and keys**. Otherwise, skip to step 9.
8. Choose the links to download your certificate PEM and private key. Save these files in a secure location on your computer.

```typescript
console.log('Loading function');
// Load the AWS SDK
var AWS = require('aws-sdk');
// Set up the code to call when the Lambda function is invoked
```

Follow the online instructions to configure your AWS IoT button.

9. Make sure that the **Enable trigger** check box is selected, and then choose **Add**. Choose **Save** in the upper right corner to save this change.

10. On the function **Configuration** page, select the name of your Lambda function. Scroll down to the **Function code** section of the page. Replace the existing code with the following:

```typescript
console.log('Loading function');
// Load the AWS SDK
var AWS = require('aws-sdk');
// Set up the code to call when the Lambda function is invoked
```
exports.handler = (event, context, callback) => {
    // Load the message passed into the Lambda function into a JSON object
    var eventText = JSON.stringify(event, null, 2);

    // Log a message to the console, you can view this text in the Monitoring tab in the Lambda console or in the CloudWatch Logs console
    console.log("Received event:", eventText);

    // Create a string extracting the click type and serial number from the message sent by the AWS IoT button
    var messageText = "Received " + event.clickType + " message from button ID: " + event.serialNumber;

    // Write the string to the console
    console.log("Message to send: " + messageText);

    // Create an SNS object
    var sns = new AWS.SNS();

    // Populate the parameters for the publish operation
    // - Message : the text of the message to send
    // - TopicArn : the ARN of the Amazon SNS topic to which you want to publish
    var params = {
        Message: messageText,
    };

    sns.publish(params, context.done);
};

Note
Replace the value of TopicArn with the ARN of the Amazon SNS topic you created previously.

Choose Save in the upper right corner to save this change.

Test Your Lambda Function

To test the Lambda function:

1. On the upper right corner of the function Configuration page, choose Test. If you haven't created a test, the Configure test event page appears. Otherwise, that page will appear as an option in the drop-down menu between the Actions menu and the Test button.

2. Copy and paste the following JSON into the Configure test event page, and then choose Save.

```json
{
    "serialNumber": "ABCDEFG12345",
    "clickType": "SINGLE",
    "batteryVoltage": "2000 mV"
}
```
3. Choose the **Test** button again to run the test. In the AWS Lambda console, scroll to the bottom of the page. The **Log output** section displays the output the Lambda function has written to the console.
Creating a Lambda Rule

Now that you have created a Lambda function, you can create a rule that invokes the Lambda function.

1. In the AWS IoT console, in the left navigation pane, choose Act.

3. Type a name and description for the rule.

4. Enter the following settings for the rule:
5. In **Set one or more actions**, choose **Add action**.

6. On the **Select an action** page, select **Invoke a Lambda function passing the message data**, and then choose **Configure action**.
7. From the **Function name** drop-down list, choose your Lambda function name, then choose **Add action**.

8. Choose **Create rule** to create your Lambda function.

---

**Test Your Lambda Rule**

In this tutorial, we assume you have completed the [AWS IoT Getting Started Tutorial (p. 5)](#), which covers:
• Configuring an AWS IoT button.
• Creating and subscribing to an Amazon SNS topic with a cell phone number.

Now that your button is configured and connected to Wi-Fi and you have configured an Amazon SNS topic, you can press the button to test your Lambda rule. You should receive an SMS text message on your phone that contains:

• The serial number of your button.
• The type of button press (SINGLE or DOUBLE).
• The battery voltage.

The message should look like the following:

```
IOT BUTTON> {
   "serialNumber" : "ABCDEFG12345",
   "clickType" : "SINGLE",
   "batteryVoltage" : "2000 mV"
}
```

If you do not have a button, you can buy one here or you can use the AWS IoT MQTT client instead.

1. In the AWS IoT console, choose Test.

2. On the MQTT client page, in the Publish section, in Specify a topic, type `iotbutton/ABCDEFG12345`.

   In Payload, type the following JSON, and then choose Publish to topic.

   ```
   {
   "serialNumber" : "ABCDEFG12345",
   "clickType" : "SINGLE",
   "batteryVoltage" : "2000 mV"
   }
   ```
3. You should receive a message on your cell phone.

Creating an Amazon SNS Rule

You can define a rule that sends message data to an Amazon SNS topic. In this tutorial, you will create a rule that sends the name of the AWS IoT thing that triggered the rule to all subscribers of an Amazon SNS topic.

To create a rule with an SNS action:

1. In the AWS IoT console, in the left navigation pane, choose Act.

3. Type a name for your rule.

4. Under **Message source**, for **Attribute** type *, topic(3). For **Topic filter**, type $aws/things/+\/
shadows/\update/\accepted. The topic filter specifies the topics that, when a message is published
to them, trigger the rule's action. The + used in the topic filter is a wildcard character that matches
any thing name. The attribute appends the thing name onto the message contents.
5. In the **Set one or more actions** section, choose **Add action**.

6. Under **Select an action**, select **Send a message as an SNS push notification**, and then choose **Configure action**. (This button is not shown in screenshot).
7. Choose **Create new topic**.

8. A new tab opens in your browser. Type a name and description for your SNS topic, and then choose **Create topic**.
9. Switch to the browser tab where the AWS IoT console is open. For **SNS target**, choose the SNS topic you just created. For **Message format**, choose **JSON**.

10. For **IAM role name**, choose **Create a new role**.
11. Type a name for the role, and then choose **Create a new role.**
12. Select the role you just created, and then choose **Add action**.
13. Choose **Create rule**.

You have now created the rule. To test the rule, add a subscription to the SNS topic you created, and update the shadow of any AWS IoT thing. You can use the AWS IoT console to find a thing, open its detail page, and change the device's shadow. When the Device Shadow service is notified of the change, it will publish a message on `$aws/things/MySNSThing/shadow/update/accepted`. Your rule is triggered and all subscribers to your SNS topic receive a message that contains your thing's name.
AWS IoT SDK Tutorials

The AWS IoT Device SDKs help you to easily and quickly connect your devices to AWS IoT. The AWS IoT Device SDKs include open-source libraries, developer guides with samples, and porting guides so that you can build innovative IoT products or solutions on your choice of hardware platforms.

This guide provides step-by-step instructions for connecting your Raspberry Pi to the AWS IoT platform and setting it up for use with the AWS IoT Embedded C SDK and Device SDK for Javascript. After following the steps in this guide, you are able to connect to the AWS IoT platform and run sample apps included with these AWS IoT SDKs.

Contents
- Connecting Your Raspberry Pi (p. 88)
- Using the AWS IoT Embedded C SDK (p. 97)
- Using the AWS IoT Device SDK for JavaScript (p. 99)

Connecting Your Raspberry Pi

Follow these steps to connect your Raspberry Pi to the AWS IoT platform.

Prerequisites
- A fully set up Raspberry Pi board with Internet access
  For information about setting up your Raspberry Pi, see Raspberry Pi Quickstart Guide.
- Chrome or Firefox (Iceweasel) browser
  For information about installing Iceweasel, see the instructions on the Embedded Linux wiki.

In this guide, the following hardware and software are used:
- Raspberry Pi 2 Model B
- Raspbian Wheezy
- Raspbian Jessie
- Iceweasel browser

Sign in to the AWS IoT Console

1. Turn on your Raspberry Pi and confirm you have an Internet connection.
3. If this is your first time using the AWS IoT console, you see the Welcome to the AWS IoT Console page. In the left navigation pane, choose Manage to expand the choices, and then choose Things.

4. On the page that says You don't have any things yet, choose Register a thing. (If you have created a thing before, choose Create.)
Create and Attach a Thing (Device)

A thing represents a device whose status or data is stored in the AWS Cloud. This stored status or data is called the device's shadow. The Device Shadow service maintains a shadow for each device connected to AWS IoT.

1. Type a name for the thing, and then choose Create thing.

2. On the Details page, choose Interact.

4. Choose Create certificate. This generates an X.509 certificate and key pair.
5. Create a working directory called `deviceSDK` where your files will be stored. Choose the links to download your public and private keys, certificate, and root CA and save them in the `deviceSDK` directory. Choose **Activate** to activate the X.509 certificate, then choose **Attach a policy**.

6. Choose **Create new policy**.
7. On the **Create a policy** page, in the **Name** field, type a name for the policy. In the **Action** field, type `iot:*`. In the **Resource ARN** field, type `*`. Select the **Allow** check box. This allows your Raspberry Pi to publish messages to AWS IoT.

8. Choose **Create**.
9. Choose the left arrow to return to the Policies page.

10. In the left navigation pane, under Security, choose Certificates.
11. In the box for the certificate you created, choose ... to open a drop-down menu, and then choose **Attach policy**.

12. In the Attach policies to certificate(s) dialog box, select the check box next to the policy you created, and then choose **Attach**.
13. In the box for the certificate you created, choose ... to open a drop-down menu, and then choose Attach thing.

14. In the Attach things to certificate(s) dialog box, select the check box next to the thing you created to represent your Raspberry Pi, and then choose Attach.
Using the AWS IoT Embedded C SDK

Set Up the Runtime Environment for the AWS IoT Embedded C SDK

1. Download the AWS IoT Device SDK for C from the following GitHub repository:

   ```
   git clone https://github.com/aws/aws-iot-device-sdk-embedded-C.git -b release
   ```

2. Before you can use the AWS IoT Embedded C SDK, you must download all required third-party libraries from GitHub. You can find instructions for doing this in the `deviceSDK/external_libs` folder.

Sample App Configuration

The AWS IoT Embedded C SDK includes sample apps for you to try. For simplicity, we are going to run `subscribe_publish_sample`.

1. Copy your certificate, private key, and root CA certificate into the `deviceSDK/certs` directory.

   If you did not get a copy of the root CA certificate, you can download it [here](link). Copy the root CA text from the browser, paste it into a file, and then copy it into the `deviceSDK/certs` directory.

   **Note**
   
   Device and root CA certificates are subject to expiration or revocation. If this should occur, you must copy a new CA certificate or private key and device certificate onto your device.

2. Navigate to the `deviceSDK/sample_apps/subscribe_publish_sample` directory. You must configure your personal endpoint, private key, and certificate. The personal endpoint is the REST API endpoint you noted earlier. If you don't remember the endpoint and you have access to a machine with the AWS CLI installed, you can use the `aws iot describe-endpoint` command to find your personal endpoint URL. Or, go to the AWS IoT console. Choose Registry, choose Things, and then choose the thing that represents your Raspberry Pi. On the Details page for the thing, in the left navigation pane, choose Interact. Copy everything, including ".com", from REST API endpoint.
3. Open the `aws_iot_config.h` file and, in the `//Get from console` section, update the values for the following:

- **AWS_IOT_MQTT_HOST**
  Your personal endpoint.
- **AWS_IOT_MY_THING_NAME**
  Your thing name.
- **AWS_IOT_ROOT_CA_FILENAME**
  Your root CA certificate.
- **AWS_IOT_CERTIFICATE_FILENAME**
  Your certificate.
- **AWS_IOT_PRIVATE_KEY_FILENAME**
  Your private key.

For example:

```
// Get from console
// ==============================================================
#define AWS_IOT_MQTT_HOST              "a22j5sm6o3yzc5.iot.us-east-1.amazonaws.com"
#define AWS_IOT_MQTT_PORT              8883
#define AWS_IOT_MQTT_CLIENT_ID         "MyRaspberryPi"
#define AWS_IOT_MY_THING_NAME          "MyRaspberryPi"
#define AWS_IOT_ROOT_CA_FILENAME       "root-CA.crt"
#define AWS_IOT_CERTIFICATE_FILENAME   "4bbdc778b9-certificate.pem.crt"
#define AWS_IOT_PRIVATE_KEY_FILENAME   "4bbdc778b9-private.pem.key"
// ==============================================================
```

**Run Sample Applications**

1. Compile the `subscribe_publish_sample_app` using the included makefile.
make \( -f \) Makefile

This generates an executable file.

2. Now run the subscribe_publish_sample_app. You should see output similar to the following:

Your Raspberry Pi is now connected to AWS IoT using the AWS IoT Device SDK for C.

Using the AWS IoT Device SDK for JavaScript

The easiest way to install the AWS IoT Device SDK for Node.js is to use npm. In this section we describe how to install Node and npm.
Set Up the Runtime Environment for the AWS IoT Device SDK for JavaScript

To use the AWS IoT Device SDK for JavaScript, install Node and the npm development tool on your Raspberry Pi. These packages are not installed by default.

**Note**
Before you continue, you might want to configure the keyboard mapping for your Raspberry Pi. For more information, see Configure Raspberry Pi Keyboard Mapping.

1. To add the Node repository, open a terminal and run the following command:

```
curl -sL https://deb.nodesource.com/setup_8.x | sudo -E bash -
```

2. To install Node, run

```
sudo apt-get install nodejs
```

3. Run `npm -v` to determine if npm is installed. If no version information is returned, install npm as follows:

```
sudo apt-get install npm
```

You should see output similar to the following:

4. To verify the installation of Node and npm, run the following:

```
node -v
```

and

```
npm -v
```

You should see output similar to the following:
Install the AWS IoT Device SDK for JavaScript

To install the AWS IoT Device SDK for JavaScript/Node.js on your Raspberry Pi, open a console window and from your ~/deviceSDK directory, use npm to install the SDK:

```bash
npm install aws-iot-device-sdk
```

After the installation is complete, you should find a node_modules directory in your ~/deviceSDK directory.

Prepare to Run the Sample Applications

The AWS IoT Device SDK for JavaScript includes sample apps for you to try. To run them, you must configure your certificates and private key.

Edit the file ~/deviceSDK/node_modules/aws-iot-device-sdk/examples/lib/cmdline.js to change the default names for the private key (privateKey), certificate (clientCert), and CA root certificate (caCert) used by the samples. For example:

```javascript
default: { 
  region: 'us-east-1',
  clientId: clientIdDefault,
  privateKey: '4bbdc77b9-private.pem.key',
  clientCert: '4bbdc77b9-certificate.pem.crt',
  caCert: 'root-CA.crt',
  testMode: 1,
  reconnectPeriod: 3 * 1000, /* milliseconds */
  delay: 4 * 1000 /* milliseconds */
};
```

Run the Sample Applications

Run the examples using

```bash
```
Run the Sample Applications

node examples/<YourDesiredExample>.js -f <certs location> -H <PREFIX>.iot.<REGION>.amazonaws.com

Assuming you are in the directory ~/deviceSDK/node_modules/aws-iot-device-sdk/, the certificates location should be ~/deviceSDK/certs/. Use the REST endpoint of your Raspberry Pi as the value of the -H parameter.

To see all available command line parameters for each sample, run the program and specify the '-h' parameter:

node examples/<YourDesiredExample>.js -h

For more information about how you can use command line options to specify the certificates location and your own host address, see the Certificates section of the AWS IoT Device SDK for JavaScript Readme on GitHub. The sample descriptions that follow this section of the Readme show additional command line parameters that are required for each sample.

If you want to create a configuration file for use with the command line option --configuration-file (-F), create a file (in JSON format) with the following properties. For example:

```
{
    "host": "a22j5sm6o3ycz5.iot.us-east-1.amazonaws.com",
    "port": 8883,
    "clientId": "MyRaspberryPi",
    "thingName": "MyRaspberryPi",
    "caCert": "root-CA.crt",
    "clientCert": "4bbdc778b9-certificate.pem.crt",
    "privateKey": "4bbdc778b9-private.pem.key"
}
```

Your Raspberry Pi is now connected to AWS IoT using the AWS IoT SDK for JavaScript.
Managing Devices with AWS IoT

AWS IoT provides a registry that helps you manage things. A thing is a representation of a specific device or logical entity. It can be a physical device or sensor (for example, a light bulb or a switch on a wall). It can also be a logical entity like an instance of an application or physical entity that does not connect to AWS IoT but is related to other devices that do (for example, a car that has engine sensors or a control panel).

Information about a thing is stored in the registry as JSON data. Here is an example thing:

```json
{
    "version": 3,
    "thingName": "MyLightBulb",
    "defaultClientId": "MyLightBulb",
    "thingTypeName": "LightBulb",
    "attributes": {
        "model": "123",
        "wattage": "75"
    }
}
```

Things are identified by a name. Things can also have attributes, which are name-value pairs you can use to store information about the thing, such as its serial number or manufacturer.

A typical device use case involves the use of the thing name as the default MQTT client ID. Although we do not enforce a mapping between a thing’s registry name and its use of MQTT client IDs, certificates, or shadow state, we recommend you choose a thing name and use it as the MQTT client ID for both the registry and the Device Shadow service. This provides organization and convenience to your IoT fleet without removing the flexibility of the underlying device certificate model or shadows.

You do not need to create a thing in the registry to connect a device to AWS IoT. Adding things to the registry allows you to manage and search for devices more easily.

How to Manage Things with the Registry

You use the AWS IoT console or the AWS CLI to interact with the registry. The following sections show how to use the CLI to work with the registry.

Create a thing

The following command shows how to use the AWS IoT CreateThing command from the CLI to create a thing:

```
$ aws iot create-thing --thing-name "MyLightBulb" --attribute-payload "{"attributes": {"wattage":"75", "model":"123"}}"
```

The CreateThing command will display the name and ARN of your new thing:

```
{
    "thingArn": "arn:aws:iot:us-east-1:123456789012:thing/MyLightBulb",
    "thingName": "MyLightBulb"
}
```
List things

You can use the ListThings command to list all things in your account:

```
$ aws iot list-things
{
    "things": [
        {
            "attributes": {,
                "model": "123",
                "wattage": "75"
            },
            "version": 1,
            "thingName": "MyLightBulb"
        },
        {
            "attributes": {,
                "numOfStates": "3"
            },
            "version": 11,
            "thingName": "MyWallSwitch"
        }
    ]
}
```

Search for things

You can use the DescribeThing command to list information about a thing:

```
$ aws iot describe-thing --thing-name "MyLightBulb"
{
    "version": 3,
    "thingName": "MyLightBulb",
    "thingArn": "arn:aws:iot:us-east-1:123456789012:thing/MyLightBulb",
    "thingId": "12345678abcdefgh12345678ijklmnop12345678",
    "defaultClientId": "MyLightBulb",
    "thingTypeName": "StopLight",
    "attributes": {
        "model": "123",
        "wattage": "75"
    }
}
```

You can use the ListThings command to search for all things associated with a thing type name:

```
$ aws iot list-things --thing-type-name "LightBulb"
{
    "things": [
        {
            "thingTypeName": "LightBulb",
            "attributes": {
                "model": "123",
                "wattage": "75"
            }
        }
    ]
}
```
You can use the `ListThings` command to search for all things that have an attribute with a specific value:

```
$ aws iot list-things --attribute-name "wattage" --attribute-value "75"
```

```
{
  "things": [
    {
      "thingTypeName": "StopLight",
      "attributes": {
        "model": "123",
        "wattage": "75"
      },
      "version": 3,
      "thingName": "MyLightBulb"
    },
    {
      "thingTypeName": "LightBulb",
      "attributes": {
        "model": "123",
        "wattage": "75"
      },
      "version": 1,
      "thingName": "MyRGBLight"
    },
    {
      "thingTypeName": "LightBulb",
      "attributes": {
        "model": "123",
        "wattage": "75"
      },
      "version": 1,
      "thingName": "MySecondLightBulb"
    }
  ]
}
```

**Update a thing**

You can use the `UpdateThing` command to update a thing:

```
$ aws iot update-thing --thing-name "MyLightBulb" --attribute-payload "{"attributes": {"wattage": "150", "model": "456"}}"
```

```
{
  "thingName": "MyLightBulb",
  "thingTypeName": "LightBulb",
  "attributes": {
    "wattage": "150",
    "model": "456"
  },
  "version": 3
}
```
Delete a thing

You can use the DeleteThing command to delete a thing:

```
$ aws iot delete-thing --thing-name "MyThing"
```

Attach a principal to a thing

A physical device must have an X.509 certificate in order to communicate with AWS IoT. You can associate the certificate on your device with the thing in the registry that represents your device. To attach a certificate to your thing, use the AttachThingPrincipal command:

```
$ aws iot attach-thing-principal --thing-name "MyLightBulb" --principal "arn:aws:iot:us-east-1:123456789012:cert/a0c01f5835079de0a7514643d68ef8414ab739ae94ee4162977b02b12842847"
```

The AttachThingPrincipal command does not produce any output.

Detach a principal from a thing

You can use the DetachThingPrincipal command to detach a certificate from a thing:

```
$ aws iot detach-thing-principal --thing-name "MyLightBulb" --principal "arn:aws:iot:us-east-1:123456789012:cert/a0c01f5835079de0a7514643d68ef8414ab739ae94ee4162977b02b12842847"
```

The DetachThingPrincipal command does not produce any output.

Thing Types

Thing types allow you to store description and configuration information that is common to all things associated with the same thing type. This simplifies the management of things in the registry. For example, you can define a LightBulb thing type. All things associated with the LightBulb thing type share a set of attributes: serial number, manufacturer, and wattage. When you create a thing of type LightBulb (or change the type of an existing thing to LightBulb) you can specify values for each of the attributes defined in the LightBulb thing type.

Although thing types are optional, their use provides better discovery of things.

- Things with a thing type can have up to 50 attributes.
- Things without a thing type can have up to three attributes.
- A thing can only be associated with one thing type.
There is no limit on the number of thing types you can create in your account.

Thing types are immutable. You cannot change a thing type name after it has been created. You can deprecate a thing type at any time to prevent new things from being associated with it. You can also delete thing types that have no things associated with them.

Create a Thing Type

You can use the `create-thing-type` command to create a thing type:

```
$ aws iot create-thing-type
  --thing-type-name "LightBulb" --thing-type-properties
    "thingTypeDescription=light bulb type, searchableAttributes=wattage,model"
```

The `create-thing-type` command returns a response that contains the thing type and its ARN:

```
{
  "thingTypeName": "LightBulb",
  "thingTypeArn": "arn:aws:iot:us-west-2:123456789012:thingtype/LightBulb"
}
```

List thing types

You can use the `list-thing-types` command to list thing types:

```
$ aws iot list-thing-types
```

The `list-thing-types` command returns a list of the thing types defined in your AWS account:

```
{
  "thingTypes": [
    {
      "thingTypeName": "LightBulb",
      "thingTypeProperties": {
        "searchableAttributes": ["wattage", "model"],
        "thingTypeDescription": "light bulb type"
      },
      "thingTypeMetadata": {
        "deprecated": false,
        "creationDate": 1468423800950
      }
    }
  ]
}
```

Describe a thing type

You can use the `describe-thing-type` command to get information about a thing type:

```
$ aws iot describe-thing-type --thing-type-name "LightBulb"
```

The `describe-thing-type` command responds with information about the specified type:
Associate a thing type with a thing

You can use the CreateThing command to specify a thing type when you create a thing:

```
$ aws iot create-thing --thing-name "MySecondLightBulb" --thing-type-name "LightBulb" --attribute-payload "{"attributes": {"wattage":"75", "model":"123"}}"
```

You can use the UpdateThing command at any time to change the thing type associated with a thing:

```
$ aws iot update-thing --thing-name "MyLightBulb" --thing-type-name "StopLight" --attribute-payload "{"attributes": {"wattage":"75", "model":"123"}}"
```

You can also use the UpdateThing command to disassociate a thing from a thing type.

Deprecate a thing type

Thing types are immutable. They cannot be changed after they are defined. You can, however, deprecate a thing type to prevent users from associating any new things with it. All existing things associated with the thing type will be unchanged.

To deprecate a thing type, use the DeprecateThingType command:

```
$ aws iot deprecate-thing-type --thing-type-name "myThingType"
```

You can use the DescribeThingType command to see the result:

```
$ aws iot describe-thing-type --thing-type-name "StopLight"
```

```json
{
    "thingTypeName": "StopLight",
    "thingTypeProperties": {
        "searchableAttributes": [
            "wattage",
            "model"
        ],
        "thingTypeDescription": "traffic light type",
    },
    "thingTypeMetadata": {
        "deprecated": true,
        "creationDate": 1468425854308,
        "deprecationDate": 1468446026349
    }
}
```
Delete a thing type

You can delete thing types only after they have been deprecated. To delete a thing type, use the 
DeleteThingType command:

```bash
$ aws iot delete-thing-type --thing-type-name "StopLight"
```

**Note**
You must wait five minutes after you deprecate a thing type before you can delete it.

**Thing Groups**

Thing groups allow you to manage several things at once by categorizing them into groups. Groups can also contain groups — you can build a hierarchy of groups. You can attach a policy to a parent group and it will be inherited by its child groups, and by all of the things in the group and in its child groups as well. This makes control of permissions easy for large numbers of things.

Here are the things you can do with thing groups:

- Create, describe or delete a group.
- Add a thing to a group, or to more than one group.
- Remove a thing from a group.
- List the groups you have created.
- List all child groups of a group (its direct and indirect descendants.)
- List the things in a group, including all the things in its child groups.
- List all ancestor groups of a group (its direct and indirect parents.)
- Add, delete or update the attributes of a group. (Attributes are name-value pairs you can use to store information about a group.)
- Attach or detach a policy to or from a group.
- List the policies attached to a group.
- List the policies inherited by a thing (by virtue of the policies attached to its group, or one of its parent groups.)
- Configure logging options for things in a group (see Configure AWS IoT Logging (p. 554).)
- Create jobs that will be sent to and executed on every thing in a group and its child groups (see Jobs (p. 281).)

Here are some limitations of thing groups:

- If a group will be a child of another group, this must be specified at the time it is created.
- You can’t change a group’s parent later. (So be sure to plan your group hierarchy and create a parent group before creating any child groups it will contain.
- You cannot add a thing to more than than 10 groups.
- You cannot add a thing to more than one group in the same hierarchy. (In other words, you cannot add a thing to two groups which share a common parent.)
- You cannot rename a group.
- Thing group names can’t contain international characters, such as ũ, é and ñ.

Attaching and detaching policies to groups can enhance the security of your AWS IoT operations in a number of significant ways. The per device method of attaching a policy to a certificate, which is then attached to a thing, is time consuming and makes it difficult to quickly update or change policies across a fleet of devices. Having a policy attached to the thing’s group saves steps when it is time to rotate the certificates on a thing. And policies are dynamically applied to things when they change group membership, so you aren’t required to re-create a complex set of permissions each time a device changes membership in a group.

### Create a Thing Group

You can use the CreateThingGroup command to create a thing group:

```
$ aws iot create-thing-group --thing-group-name LightBulbs
```

The CreateThingGroup command returns a response that contains the thing group, its ID, and its ARN:

```
{
  "thingGroupName": "LightBulbs",
  "thingGroupId": "abcdefgh12345678ijklmnop12345678qrstuvwx",
  "thingGroupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/LightBulbs"
}
```

Here is an example which specifies a parent of the thing group when it is created:

```
$ aws iot create-thing-group --thing-group-name RedLights --parent-group-name LightBulbs
```

As before, the CreateThingGroup command returns a response that contains the thing group and its ID and ARN:
Describe a thing group

You can use the DescribeThingGroup command to get information about a thing group:

```bash
# aws iot describe-thing-group --thing-group-name RedLights
```

The DescribeThingGroup command responds with information about the specified group:

```json
{
  "thingGroupName": "RedLights",
  "thingGroupId": "12345678abcdefgh12345678ijklmnop12345678",
  "version": 1,
  "thingGroupMetadata": {
    "creationDate": 1478299948.882,
    "parentGroupName": "Lights",
    "rootToParentThingGroups": [
      {
        "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/ShinyObjects",
        "groupName": "ShinyObjects"
      },
      {
        "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/LightBulbs",
        "groupName": "LightBulbs"
      }
    ]
  },
  "thingGroupProperties": {
    "attributePayload": {
      "attributes": {
        "brightness": "3400 lumens"
      }
    },
    "thingGroupDescription": "string"
  }
}
```

Add thing to thing group

You can use the AddThingToThingGroup command to add a thing to a group:

```json
{  "thingGroupName": "RedLights",
  "thingGroupId": "abcdefgh12345678ijklmnop12345678qrstuvwx",
}
```

**Important**

Keep in mind the following limits when creating group hierarchies:

- A group can have at most one direct parent.
- A group may have no more than 100 direct child groups.
- The maximum depth of a group hierarchy is 7.
- A group can have up to 50 attributes. (Attributes are name-value pairs you can use to store information about a group.) Each attribute name can contain up to 128 characters and each value up to 800 characters.
Remove thing from thing group

You can use the RemoveThingFromThingGroup command to remove a thing from a group:

```bash
$ aws iot remove-thing-from-thing-group --thing-name MyLightBulb --thing-group-name RedLights
```

The RemoveThingFromThingGroup command does not produce any output.

### List things in thing group

You can use the ListThingsInThingGroup command to list the things belonging to a group:

```bash
$ aws iot list-things-in-thing-group --thing-group-name LightBulbs
```

The ListThingsInThingGroup command returns a list of the things in the given group:

```json
{
  "things": [
    "TestThingA"
  ]
}
```

With the `--recursive` parameter, you can list things belonging to a group and those in any of its child groups as well:

```bash
$ aws iot list-things-in-thing-group --thing-group-name LightBulbs --recursive
```

```json
{
  "things": [
    "TestThingA",
    "MyLightBulb"
  ]
}
```

**Note**

This operation is eventually consistent, in other words, changes to the thing group may not be reflected immediately.

### List thing groups

You can use the ListThingGroups command to list groups you have created:

```bash
$ aws iot list-thing-groups
```
The `ListThingGroups` command returns a list of the groups defined in your AWS account:

```
{
  "thingGroups": [ 
  
    { "groupName": "LightBulbs",  
      "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/LightBulbs"  
    },  
    { "groupName": "RedLights",  
      "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/RedLights"  
    },  
    { "groupName": "RedLEDLights",  
      "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/RedLEDLights"  
    },  
    { "groupName": "RedIncandescentLights",  
      "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/RedIncandescentLights"  
    },  
    { "groupName": "ReplaceableObjects",  
      "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/ReplaceableObjects"  
    } 
  ]
}
```

Use the optional filters to list those groups that have a given group as parent (`--parent-group`) or groups whose name begins with a given prefix (`--name-prefix-filter`). The `--recursive` parameter allows you to list all children groups as well, not just direct children:

```
$ aws iot list-thing-groups --parent-group LightBulbs
```

In this case, the `ListThingGroups` command returns a list of the direct child groups of the thing group defined in your AWS account:

```
{
  "childGroups": [ 
  
    { "groupName": "RedLights",  
      "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/RedLights"  
    } 
  ]
}
```

Use the `--recursive` parameter with the `ListThingGroups` command to list all child groups of a thing group, not just direct children:

```
$ aws iot list-thing-groups --parent-group LightBulbs --recursive
```

The `ListThingGroups` command returns a list of all child groups of the thing group:

```
{
  "childGroups": [ 
  
    { "groupName": "RedLights",  
      "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/RedLights"  
    } 
  ]
}
```
Note
This operation is eventually consistent, in other words, changes to the thing group may not be reflected immediately.

List groups for thing

You can use the `ListThingGroupsForThing` command to list the groups a thing belongs to, including any parent groups:

```
$ aws iot list-thing-groups-for-thing --thing-name MyLightBulb
```

The `ListThingGroupsForThing` command returns a list of the thing groups this thing belongs to, including any parent groups:

```
{
    "thingGroups": [
        {
            "groupName": "LightBulbs",
            "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/LightBulbs"
        },
        {
            "groupName": "RedLights",
            "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/RedLights"
        },
        {
            "groupName": "ReplaceableObjects",
            "groupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/ReplaceableObjects"
        }
    ]
}
```

Update a Thing Group

You can use the `UpdateThingGroup` command to update the attributes of a thing group:

```
$ aws iot update-thing-group --thing-group-name "LightBulbs" --thing-group-properties "thingGroupDescription="this is a test group\", attributePayload=\"{"attributes \"="{"Owner\"="150\",\"modelNames\"="456\"}}"
```

The `UpdateThingGroup` command returns a response that contains the group's version number after the update:

```
{
    "version": 4
}
```
Delete a thing group

To delete a thing group, use the `DeleteThingGroup` command:

```
$ aws iot delete-thing-group --thing-group-name "RedLights"
```

The `DeleteThingGroup` command does not produce any output.

**Important**

If you try to delete a thing group which has child thing groups, this will generate an error:

```
A client error (InvalidRequestException) occurred when calling the
DeleteThingGroup
operation: Cannot delete thing group : RedLights when there are still child groups
attached to it.
```

You must delete any child groups first before deleting the group.

You can delete a group that has child things, but any permissions granted to the things by membership in the group will no longer apply. Before deleting a group that has a policy attached, check carefully that removing those permissions would not stop the things in the group from being able to function properly. Also, note that commands that show which groups a thing belongs to (for example, `ListGroupsForThing`) may continue to show the group while records in the cloud are being updated.

Attach a policy to a thing group

You can use the `AttachPolicy` command to attach a policy to a thing group and so, by extension, to all things in that group and things in any of its child groups:

```
$ aws iot attach-policy \
--target "arn:aws:iot:us-west-2:123456789012:thinggroup/LightBulbs" \ 
--policy-name "myLightBulbPolicy"
```

The `AttachPolicy` command does not produce any output.

**Important**

The maximum number of policies that can be attached to a group is 2.

The `--target` parameter can be a thing group ARN (as above), a certificate ARN, or an Amazon Cognito Identity. See Security and Identity for AWS IoT (p. 119) for more information about policies, certificates and authentication.

Detach a policy from a thing group

You can use the `DetachPolicy` command to detach a policy from a group and so, by extension, to all things in that group and things in any of its child groups:

```
$ aws iot detach-policy --target "arn:aws:iot:us-west-2:123456789012:thinggroup/LightBulbs" \ 
--policy-name "myLightBulbPolicy"
```

The `DetachPolicy` command does not produce any output.

**Note**

A group can have up to 50 attributes.
List the policies attached to a thing group

You can use the `ListAttachedPolicies` command to list the policies attached to a group:

```bash
```

The `--target` parameter can be a thing group ARN (as above), a certificate ARN, or an Amazon Cognito Identity.

Add the optional `--recursive` parameter to include all policies attached to the group's parent groups as well.

The `ListAttachedPolicies` command returns a list of policies:

```json
{
  "policies": [
    "MyLightBulbPolicy"
  ]
}
```

List the groups for a policy

You can use the `ListTargetsForPolicy` command to list the targets, including any groups, that a policy is attached to:

```bash
$ aws iot list-targets-for-policy --policy-name "MyLightBulbPolicy"
```

Add the optional `--page-size number` parameter to specify the maximum number of results to be returned for each query, and the `--marker string` parameter on subsequent calls to retrieve the next set of results, if any.

The `ListTargetsForPolicy` command returns a list of targets and the token to use to retrieve more results:

```json
{
  "nextMarker": "string",
  "targets": [ "string" ... ]
}
```

Get effective policies for a thing

You can use the `GetEffectivePolicies` command to list the policies in effect for a thing, including the policies attached to any groups the thing belongs to (whether the group is a direct parent or indirect ancestor):

```bash
$ aws iot get-effective-policies \
  --thing-name "MyLightBulb" \
  --principal "arn:aws:iot:us-east-1:123456789012:cert/a0c0f5835079de0a7514643d68ef8414ab739a1e94ee4162977b02b12842847"
```

Use the `--principal` parameter to specify the ARN of the certificate attached to the thing. If you are using Amazon Cognito Identity authentication, use the `--cognito-identity-pool-id` parameter
and, optionally, add the --principal parameter to specify a specific Cognito Identity. (If you specify only the --cognito-identity-pool-id then the policies associated with that identity pool's role for unauthenticated users are returned. If you use both, the policies associated with that identity pool's role for authenticated users are returned.

The --thing-name parameter is optional and may be used instead of the --principal parameter. When used, the policies attached to any group the thing belongs to, and the policies attached to any parent groups of these groups (up to the root group in the hierarchy) will be returned.

The GetEffectivePolicies command returns a list of policies:

```json
{
  "effectivePolicies": [
    {
      "policyArn": "string",
      "policyDocument": "string",
      "policyName": "string"
    },
    ...
  ]
}
```

**Test authorization for MQTT actions**

You can use the TestAuthorization command to test whether an MQTT action is allowed for a thing:

```bash
$ aws iot test-authorization \
--principal "arn:aws:iot:us-east-1:123456789012:cert/a0c01f5835079de0a7514643d68ef8414ab739a1e94ee4162977b02b12842847" \
--auth-infos "[ { "actionType": "PUBLISH", "resources": [ "arn:aws:iot:us-east-1:123456789012:topic/iotButton/G030JF053216F1BS" ] } ]"
```

Use the --principal parameter to specify the ARN of the certificate attached to the thing. If using Amazon Cognito Identity authentication, specify a Cognito Identity as the --principal or use the --cognito-identity-pool-id parameter, or both. (If you specify only the --cognito-identity-pool-id then the policies associated with that identity pool's role for unauthenticated users are considered. If you use both, the policies associated with that identity pool's role for authenticated users are considered.

Specify one or more MQTT actions you want to test by listing sets of resources and action types following the --auth-infos parameter. The actionType field should contain "PUBLISH", "SUBSCRIBE", "RECEIVE", or "CONNECT". The resources field should contain a list of resource ARNs. See AWS IoT Policies (p. 132) for more information.

You can test the effects of adding policies by specifying them with the --policy-names-to-add parameter. Or you can test the effects of removing policies by them with the --policy-names-to-skip parameter.

You can use the optional --client-id parameter to further refine your results.

The TestAuthorization command returns details on actions which were allowed or denied for each set of --auth-infos queries you specified:

```json
{
  "authResults": [
    {
      "allowed": {
        "policies": [ ...
```


```
{
    "policyArn": "string",
    "policyName": "string"
  },
  "authDecision": "string",
  "authInfo": {
    "actionType": "string",
    "resources": [ "string" ]
  },
  "denied": {
    "explicitDeny": {
      "policies": [
        {
          "policyArn": "string",
          "policyName": "string"
        }
      ]
    },
    "implicitDeny": {
      "policies": [
        {
          "policyArn": "string",
          "policyName": "string"
        }
      ]
    }
  },
  "missingContextValues": [ "string" ]
}
```
Security and Identity for AWS IoT

Each connected device must have a credential to access the message broker or the Device Shadow service. All traffic to and from AWS IoT must be encrypted over Transport Layer Security (TLS). Device credentials must be kept safe in order to send data securely to the message broker. AWS Cloud security mechanisms protect data as it moves between AWS IoT and other devices or AWS services.

- You are responsible for managing device credentials (X.509 certificates, AWS credentials) on your devices and policies in AWS IoT. You are responsible for assigning unique identities to each device and managing the permissions for a device or group of devices.
- Devices connect using your choice of identity (X.509 certificates, IAM users and groups, Amazon Cognito identities, or custom authentication tokens) over a secure connection according to the AWS IoT connection model.
- When using AWS IoT authentication, the message broker authenticates and authorizes all actions in your account. The message broker is responsible for authenticating your devices, securely ingesting device data, and adhering to the access permissions you place on devices using policies.
- When using custom authentication, a custom authorizer is responsible for authenticating your devices and providing an AWS IoT/IAM policy to authorize actions in your account.
- The AWS IoT rules engine forwards device data to other devices and other AWS services according to rules you define. It uses AWS access management systems to securely transfer data to its final destination.

AWS IoT Authentication

AWS IoT supports four types of identity principals for authentication:

- X.509 certificates
- IAM users, groups, and roles
- Amazon Cognito identities
- Federated identities

These identities can be used with mobile applications, web applications, or desktop applications. They can even be used by a user typing AWS IoT CLI commands. Typically, AWS IoT devices use X.509...
certificates, while mobile applications use Amazon Cognito identities. Web and desktop applications use IAM or federated identities. CLI commands use IAM.

**X.509 Certificates**

X.509 certificates are digital certificates that use the X.509 public key infrastructure standard to associate a public key with an identity contained in a certificate. X.509 certificates are issued by a trusted entity called a certification authority (CA). The CA maintains one or more special certificates called CA certificates that it uses to issue X.509 certificates. Only the certification authority has access to CA certificates.

*Note*

We recommend that each device be given a unique certificate to enable fine-grained management including certificate revocation. Devices must support rotation and replacement of certificates in order to ensure smooth operation as certificates expire.

AWS IoT supports the following certificate-signing algorithms:

- SHA256WITHRSA
- SHA384WITHRSA
- SHA384WITHRSA
- SHA512WITHRSA
- RSASSAPSS
- DSA_WITH_SHA256
- ECDSA-WITH-SHA256
- ECDSA-WITH-SHA384
- ECDSA-WITH-SHA512

Certificates provide several benefits over other identification and authentication mechanisms. Certificates enable asymmetric keys to be used with devices. This means you can burn private keys into secure storage on a device. This way, sensitive cryptographic material never leaves the device. Certificates provide stronger client authentication over other schemes, such as user name and password or bearer tokens, because the secret key never leaves the device.

AWS IoT authenticates certificates using the TLS protocol’s client authentication mode. TLS is available in many programming languages and operating systems and is commonly used for encrypting data. In TLS client authentication, AWS IoT requests a client X.509 certificate and validates the certificate’s status and AWS account against a registry of certificates. It then challenges the client for proof of ownership of the private key that corresponds to the public key contained in the certificate.

To use AWS IoT certificates, clients must support all of the following in their TLS implementation:

- TLS 1.2.
- SHA-256 RSA certificate signature validation.
- One of the cipher suites from the TLS cipher suite support section.

**X.509 Certificates and AWS IoT**

AWS IoT can use AWS IoT-generated certificates or certificates signed by a CA certificate for device authentication. Certificates generated by AWS IoT are long-lived (but will expire at 2049-12-31T23:59:59Z, that is at midnight GMT on December 31, 2049.) The expiry date and time for certificates signed by a CA certificate are set when the certificate is created.
Note
We recommend that each device be given a unique certificate to enable fine-grained management including certificate revocation. Devices must support rotation and replacement of certificates in order to ensure smooth operation as certificates expire.

To use a certificate that is not created by AWS IoT, you must register a CA certificate. All device certificates must be signed by the CA certificate you register.

You can use the AWS IoT console or CLI to perform the following operations:

- Create and register an AWS IoT certificate.
- Register a CA certificate.
- Register a device certificate.
- Activate or deactivate a device certificate.
- Revoke a device certificate.
- Transfer a device certificate to another AWS account.
- List all CA certificates registered to your AWS account.
- List all device certificates registered to your AWS account.

For more information about the CLI commands to use to perform these operations, see AWS IoT CLI Reference.

For more information about using the AWS IoT console to create certificates, see Create and Activate a Device Certificate.

Server Authentication

Server certificates allow your devices to verify that they're communicating with AWS IoT and not another server impersonating AWS IoT. AWS IoT server certificates are signed by one of the following CA certificates:

- RSA 2048 bit key: VeriSign Class 3 Public Primary G5 root CA certificate
- RSA 2048 bit key: Amazon Root CA 1
- RSA 4096 bit key: Amazon Root CA 2
- ECC 256 bit key: Amazon Root CA 3
- ECC 384 bit key: Amazon Root CA 4

In order for your devices to validate the AWS IoT server certificate we recommend installing all of the CA certificates listed above on your devices.

Storing all of these certificates on your device can take up valuable memory space. If your devices implement RSA-based validation, you can omit the Amazon Root CA 3 and Amazon Root CA 4 ECC certificates. If your devices implement ECC-based certificate validation, you can omit the Amazon Root CA 1 and Amazon Root CA 2 RSA certificates.

You will need to include the VeriSign Class 3 Public Primary G5 root CA certificate regardless of the type of certificate validation your devices use.

Note
CA certificates have an expiration date after which they cannot be used to validate a server's certificate. CA certificates might have to be replaced before their expiration date. Make sure that you can update the root CA certificates on all of your devices to ensure ongoing connectivity and to keep up-to-date with security best practices.
Reference the CA root certificate in your device code when you connect to AWS IoT. For more information, see the AWS IoT Device SDKs (p. 535).

Create and Register an AWS IoT Device Certificate

You can use the AWS IoT console or the AWS IoT CLI to create an AWS IoT certificate.

To create a certificate (console)

1. Sign in to the AWS Management Console and open the AWS IoT console.
2. In the left navigation pane, choose Security to expand the choices, and then choose Certificates. Choose Create.
3. Choose One-click certificate creation - Create certificate. Alternatively, to generate a certificate with a certificate signing request (CSR), choose Create with CSR.
4. Use the links to the public key, private key, and certificate to download each to a secure location.
5. Choose Activate.

To create a certificate (CLI)

The AWS IoT CLI provides two commands to create certificates:

- create-keys-and-certificate
  - The CreateKeysAndCertificate API creates a private key, public key, and X.509 certificate.
- create-certificate-from-csr
  - The CreateCertificateFromCSR API creates a certificate given a CSR.

Use Your Own Certificate

To use your own X.509 certificates, you must register a CA certificate with AWS IoT. The CA certificate can then be used to sign device certificates. You can register up to 10 CA certificates with the same subject field per AWS account per region. This allows you to have more than one CA sign your device certificates.

Note

Device certificates must be signed by the registered CA certificate. It is common for a CA certificate to be used to create an intermediate CA certificate. If you are using an intermediate certificate to sign your device certificates, you must register the intermediate CA certificate. Use the AWS IoT root CA certificate when you connect to AWS IoT even if you register your own root CA certificate. The AWS IoT root CA certificate is used by a device to verify the identity of the AWS IoT servers.

Contents

- Registering Your CA Certificate (p. 123)
- Creating a Device Certificate Using Your CA Certificate (p. 124)
- Registering a Device Certificate (p. 125)
- Registering Device Certificates Manually (p. 125)
- Using Automatic/Just-in-Time Registration for Device Certificates (p. 125)
- Deactivate the CA Certificate (p. 126)
- Revoke the Device Certificate (p. 126)

If you do not have a CA certificate, you can use OpenSSL tools to create one.
To create a CA certificate

1. Generate a key pair.
   
   ```bash
   openssl genrsa -out rootCA.key 2048
   ```

2. Use the private key from the key pair to generate a CA certificate.
   
   ```bash
   openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem
   ```

Registering Your CA Certificate

To register your CA certificate, you must:

- Get a registration code from AWS IoT.
- Sign a private key verification certificate with your CA certificate.
- Pass your CA certificate and a private key verification certificate to the `register-ca-certificate` CLI command.

The **Common Name** field in the private key verification certificate must be set to the registration code generated by the `get-registration-code` CLI command. A single registration code is generated per AWS account. You can use the `register-ca-certificate` command or the AWS IoT console to register CA certificates.

**Note**

A CA certificate cannot be registered to more than one account in the same region. However, a CA certificate can be registered to more than one account if the accounts are in different regions.

To register a CA certificate

1. Get a registration code from AWS IoT. This code is used as the **Common Name** of the private key verification certificate.
   
   ```bash
   aws iot get-registration-code
   ```

2. Generate a key pair for the private key verification certificate.
   
   ```bash
   openssl genrsa -out verificationCert.key 2048
   ```

3. Create a CSR for the private key verification certificate. Set the **Common Name** field of the certificate to your registration code.
   
   ```bash
   openssl req -new -key verificationCert.key -out verificationCert.csr
   ```
   
   You are prompted for some information, including the **Common Name**, for the certificate.

   ```
   Country Name (2 letter code) [AU]:
   State or Province Name (full name) []:
   Locality Name (for example, city) []:
   Organization Name (for example, company) []:
   Organizational Unit Name (for example, section) []:
   Common Name (e.g. server FQDN or YOUR name) []:XXXXXXXXXXXXMYREGISTRATIONCODEXXXXXX
   Email Address []:
   ```
4. Use the CSR to create a private key verification certificate.

```bash
openssl x509 -req -in verificationCert.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out verificationCert.pem -days 500 -sha256
```

5. Register the CA certificate with AWS IoT. Pass in the CA certificate and the private key verification certificate to the `register-ca-certificate` CLI command.

```bash
aws iot register-ca-certificate --ca-certificate file://rootCA.pem --verification-cert file://verificationCert.pem
```

6. Use the `update-certificate` CLI command to activate the CA certificate.

```bash
aws iot update-ca-certificate --certificate-id xxxxxxxxxxx --new-status ACTIVE
```

Creating a Device Certificate Using Your CA Certificate

You can use a CA certificate registered with AWS IoT to create a device certificate. The device certificate must be registered with AWS IoT before use.

**To create a device certificate**

1. Generate a key pair.

```bash
openssl genrsa -out deviceCert.key 2048
```

2. Create a CSR for the device certificate.

```bash
openssl req -new -key deviceCert.key -out deviceCert.csr
```

You are prompted for some information, as shown here.

```
Country Name (2 letter code) [AU]:
State or Province Name (full name) []:
Locality Name (for example, city) []:
Organization Name (for example, company) []:
Organizational Unit Name (for example, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

3. Create a device certificate from the CSR.

```bash
openssl x509 -req -in deviceCert.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out deviceCert.pem -days 500 -sha256
```

**Note**

You must use the CA certificate registered with AWS IoT to create device certificates. If you have more than one CA certificate (with the same subject field and public key) registered in your AWS account, you must specify the CA certificate used to create the device certificate when you register your device certificate.

4. Register a device certificate.

```bash
```

5. Use the `update-certificate` CLI command to activate the device certificate.
Registering a Device Certificate

You must use the CA certificate registered with AWS IoT to sign device certificates. If you have more than one CA certificate (with the same subject field and public key) registered in your AWS account, you must specify the CA certificate used to sign the device certificate when you register your device certificate. You can register each device certificate manually, or you can use automatic registration, which allows devices to register their certificate when they connect to AWS IoT for the first time.

Registering Device Certificates Manually

Use the following CLI command to register a device certificate:

```
aws iot register-certificate --certificate-pem file://deviceCert.crt --ca-certificate-pem file://caCert.crt
```

Using Automatic/Just-in-Time Registration for Device Certificates

To register device certificates automatically when devices first connect to AWS IoT, you must enable automatic registration for your CA certificate. This registers any device certificate signed by your CA certificate when it connects to AWS IoT.

Enable Automatic Registration

Use the `update-ca-certificate` API to set the `auto-registration-status` of the CA certificate to `ENABLE`:

```
$ aws iot update-ca-certificate --certificate-id caCertificateId --new-auto-registration-status ENABLE
```

You can also set the `auto-registration-status` to `ENABLE` when you use the `register-ca-certificate` API to register your CA certificate:

```
aws iot register-ca-certificate --ca-certificate file://rootCA.pem --verification-cert file://privateKeyVerificationCert.crt --allow-auto-registration
```

When a device first attempts to connect to AWS IoT, as part of the TLS handshake, it must present a registered CA certificate and a device certificate. AWS IoT recognizes the CA certificate as a registered CA certificate and automatically registers the device certificate and sets its status to `PENDING_ACTIVATION`. This means that the device certificate was automatically registered and is awaiting activation. A certificate must be in the `ACTIVE` state before it can be used to connect to AWS IoT. When AWS IoT automatically registers a certificate or when a certificate in `PENDING_ACTIVATION` status connects, AWS IoT publishes a message to the following MQTT topic:

```
$aws/events/certificates/registered/caCertificateID
```

Where `caCertificateID` is the ID of the CA certificate that issued the device certificate.

The message published to this topic has the following structure:

```
{
```

```
You can create a rule that listens on this topic and performs some actions. We recommend that you create a Lambda rule that verifies the device certificate is not on a certificate revocation list (CRL), activates the certificate, and creates and attaches a policy to the certificate. The policy determines which resources the device is able to access. For more information about how to create a Lambda rule that listens on the $aws/events/certificates/registered/caCertificateID topic and performs these actions, see Just-in-Time Registration.

**Deactivate the CA Certificate**

When you register a device certificate, AWS checks if the associated CA certificate is ACTIVE. If the CA certificate is INACTIVE, AWS IoT does not allow the device certificate to be registered. By marking the CA certificate as INACTIVE, you prevent any new device certificates issued by the compromised CA to be registered in your account. You can use the update-ca-certificate API to deactivate the CA certificate:

```
$ aws iot update-ca-certificate --certificate-id certificateId --new-status INACTIVE
```

*Note*

Any registered device certificates that were signed by the compromised CA certificate continue to work until you explicitly revoke them.

Use the ListCertificatesByCA API to get a list of all registered device certificates that were signed by the compromised CA. For each device certificate signed by the compromised CA certificate, use the UpdateCertificate API to revoke the device certificate to prevent it from being used.

**Revoke the Device Certificate**

If you detect suspicious activity on a registered device certificate, you can use the update-certificate API to revoke it:

```
$ aws iot update-certificate --certificate-id certificateId --new-status REVOKED
```

If any error or exception occurs during the auto-registration of the device certificates, AWS IoT sends events or messages to your logs in CloudWatch Logs. For more information about setting up the logs for your account, see the Amazon CloudWatch documentation.

**IAM Users, Groups, and Roles**

IAM users, groups, and roles are the standard mechanisms for managing identity and authentication in AWS. You can use them to connect to AWS IoT HTTP interfaces using the AWS SDK and CLI.

IAM roles also allow AWS IoT to access other AWS resources in your account on your behalf. For example, if you want to have a device publish its state to a DynamoDB table, IAM roles allow AWS IoT to interact with Amazon DynamoDB. For more information, see IAM Roles.

For message broker connections over HTTP, AWS IoT authenticates IAM users, groups, and roles using the Signature Version 4 signing process. For more information, see Signing AWS API Requests.
When using AWS Signature Version 4 with AWS IoT, clients must support the following in their TLS implementation:

- TLS 1.2, TLS 1.1, TLS 1.0.
- SHA-256 RSA certificate signature validation.
- One of the cipher suites from the TLS cipher suite support section.

For information, see the IAM User Guide.

## Amazon Cognito Identities

Amazon Cognito Identity allows you to use your own identity provider or other popular identity providers, such as Login with Amazon, Facebook, or Google. You exchange a token from your identity provider for AWS security credentials. The credentials represent an IAM role and can be used with AWS IoT.

AWS IoT extends Amazon Cognito and allows policy attachment to Amazon Cognito identities. You can attach a policy to an Amazon Cognito identity and give fine-grained permissions to an individual user of your AWS IoT application. In this way, you can assign permissions between specific customers and their devices. For more information, see Amazon Cognito Identity.

### Custom Authentication

AWS IoT allows you to define custom authorizers that allow you to manage your own authentication and authorization strategy using a custom authentication service and a Lambda function. Custom authorizers allow AWS IoT to authenticate your devices and authorize operations using bearer token authentication and authorization strategies.

When an HTTP connection is established (and optionally upgraded to a WebSocket connection) and Signature Version 4 headers are not present, the AWS IoT device gateway checks if a custom authorizer is configured for the endpoint, and if so, it is used to authenticate the connection and authorize the device. Custom authorizers can implement various authentication strategies (for example: JWT verification, OAuth provider callout, and so on) and must return policy documents that are used by the device gateway to authorize MQTT operations.

### Custom Authorizers

Custom authorizers consist of:
Name

A unique arbitrary string that identifies the authorizer.

Lambda function ARN

An ARN of a Lambda function that implements the authentication logic and returns authorization policies.

Public key

The public key from a key pair that is used to prevent unauthorized calls to the authorizer's Lambda function.

Use the following command to generate a key pair: `openssl genrsa -out myKeyPair.pem 2048`. Use the following command to extract the public key from the key pair: `openssl rsa -in myKeyPair.pem -pubout > mykey.pub`

Token key name

The key name used to extract tokens from the WebSocket connection headers.

The logic that performs the authentication is implemented in a Lambda function.

**Note**

AWS Lambda usage is billed. For more information about Lambda, see [AWS Lambda Developer Guide](#).

This function takes a token presented by a device, authenticates the device, and returns the following information:

isAuthenticated

A Boolean value that indicates whether the token was authenticated. If this is `false`, the rest of the response fields should be ignored.

principalId

The principal that is getting this permission.

policyDocuments

A list of policies that specifies which operations the token bearer can perform.

DisconnectAfterInSecs

The length of time, in seconds, to keep the WebSocket connection open.

RefreshAfterInSecs

The length of time, in seconds, after which the Lambda function is invoked to refresh the policies.

Context

Additional information derived after validating the token. This information is made available in AWS IoT rules engine SQL statements and IAM/AWS IoT policy variables.

You must grant permission to the AWS IoT service principal to invoke the Lambda function that implements the custom authentication/authorization logic. You can do this with the following CLI command:

```bash
aws lambda add-permission --function-name <lambda_function_name> --statement-id <unique_identifier_string> --action 'lambda:InvokeFunction'
```
Configure a Custom Authorizer

1. Create a Lambda function that implements your authentication/authorization logic (for example, the MyAuthorizerFunction in the following step). The following is an example of what a custom authorizing Lambda function might return:

```
{
  "isAuthenticated": true,
  "principalId": "xxxxxxxx",
  "disconnectAfterInSeconds": 86400,
  "refreshAfterInSeconds": 300,
  "policyDocuments": [
    "{"Version":"2012-10-17","Statement": [{"Action":"...","Effect": "Allow|Deny","Resource":"..."}]
  ],
  "context": {
    "username": "johnDoe123",
    "city": "Seattle",
    "country": "USA"
  }
}
```

The return value of the Lambda function should be similar to the above. It can be either a JSON serialized or non-serialized object.

2. Register a custom authorizer with AWS IoT using the create-authorizer API.

```
aws iot create-authorizer --authorizer-name MyAuthorizer
  --token-key-name MyAuthorizerToken // Key to extract token from headers
  --token-signing-public-keys FIRST_KEY= -----BEGIN PUBLIC KEY-----
  [...insert your public key here...]
  -----END PUBLIC KEY----- // Key used to verify token signature

  --status ACTIVE // Authorizer status - must be ACTIVE
  --region us-west-2 // AWS region
  --endpoint https://us-west-2.iot.amazonaws.com // IoT endpoint
```

The test-invoke-authorizer API can be used to test if the custom authorizer Lambda function has been configured correctly, as shown:
aws iot test-invoke-authorizer --authorizer-name <NAME_OF_AUTHORIZER> --token <TOKEN_VALUE> --token-signature <TOKEN_SIGNATURE>

**Note**

<TOKEN_SIGNATURE> must be signed with the private key of the public/private key pair uploaded to AWS IoT used in the create-authorizer call. One method of locally creating <TOKEN_SIGNATURE> from a UNIX-like command line is as follows:

```bash
echo -n <TOKEN_VALUE> | openssl dgst -sha256 -sign <PRIVATE_KEY> | openssl base64
```

You must trim all newline characters from the result of the prior command before passing the <TOKEN_SIGNATURE> value to the test-invoke-authorizer API.

## Custom Authorizer Workflow

For a device to authenticate with the AWS IoT device gateway using a custom authorizer, it needs both a token and a signature used by AWS to validate the tokens before invoking the authorizer.

When a device attempts to connect to AWS IoT, it sends the following information in HTTP headers:

- A token generated by your authentication service.
- The signature generated by your authentication service.
- The authorizer used to authenticate the token. If omitted, the default authorizer is used.

The following is an example HTTP request to connect to AWS IoT over the WebSocket protocol.

```plaintext
GET /mqtt HTTP/1.1
Host: <your-iot-endpoint>
Upgrade: WebSocket
Connection: Upgrade
x-amz-customauthorizer-name: <authorizer-name>
x-amz-customauthorizer-signature: <token-signature>
<token-key-name>: <some-token>
sec-WebSocket-Key: <any random base64 value>
sec-websocket-protocol: mqtt
sec-WebSocket-Version: <websocket version>
```

In this example, the x-amz-customauthorizer-name header specifies the custom authorizer to use, the x-amz-customauthorizer-signature header contains the digital signature used to verify the token, and the token-key-name is the token key name specified by the --token-key-name passed to the create-authorizer API.

The AWS IoT device gateway validates the digital signature and if valid, calls the specified authorizer. The following is an example payload AWS IoT sends to the custom authenticator’s Lambda function.

```json
{
  "token": "some-token"
}
```

The authorizer validates the token and returns a principal ID, its associated AWS IoT/IAM policy, and time-to-live (TTL) information for the connection.
The following is an example of the response from a custom authorizer.

```
{
  "isAuthenticated":true,
  "principalId": "xxxxxxxx",
  "disconnectAfterInSeconds": 86400,
  "refreshAfterInSeconds": 300,
  "policyDocuments": [
  ]
}
```

The return value of the Lambda function should be similar to the above and can be either a JSON serialized or non-serialized object.

The AWS IoT device gateway then establishes the WebSocket connection. AWS IoT caches the policies associated with the principal so subsequent calls can be authorized without having to reauthenticate the device. Any failure that occurs during custom authentication results in authentication failure and connection termination.

For an end-to-end example of this workflow, see How to Use Your Own Identity and Access Management Systems to Control Access to AWS IoT Resources.

## Authorization

Policies determine what an authenticated identity can do. An authenticated identity is used by devices, mobile applications, web applications, and desktop applications. An authenticated identity can even be a user typing AWS IoT CLI commands. The identity can execute AWS IoT operations only if it has a policy that grants it permission.

Both AWS IoT policies and IAM policies are used with AWS IoT to control the operations an identity (also called a principal) can perform. The policy type you use depends on the type of identity you are using to authenticate with AWS IoT. The following table shows the identity types, the protocols they use, and the policy types that can be used for authorization.

AWS IoT operations are divided into two groups:

- Control plane API allows you to perform administrative tasks like creating or updating certificates, things, rules, and so on.
- Data plane API allows you send data to and receive data from AWS IoT.

The type of policy you use depends on whether you are using control plane or data plane API.

## AWS IoT Data Plane API and Policy Types

<table>
<thead>
<tr>
<th>Protocol and Authentication Mechanism</th>
<th>SDK</th>
<th>Identity Type</th>
<th>Policy Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>MQTT over mutual authentication (port 8883 or 443)</td>
<td>AWS IoT Device SDK</td>
<td>X.509 certificates</td>
<td>AWS IoT policy</td>
</tr>
</tbody>
</table>
AWS IoT policies are attached to X.509 certificates or Amazon Cognito identities. IAM policies are attached to an IAM user, group, or role. If you use the AWS IoT console or the AWS IoT CLI to attach the policy (to a certificate or Amazon Cognito Identity), you use an AWS IoT policy. Otherwise, you use an IAM policy.

Policy-based authorization is a powerful tool. It gives you complete control over what a device, user, or application can do in AWS IoT. For example, consider a device connecting to AWS IoT with a certificate. You can allow the device to access all MQTT topics, or you can restrict its access to a single topic. In another example, consider a user typing CLI commands at the command line. By using a policy, you can allow or deny access to any command or AWS IoT resource for the user. You can also control an application's access to AWS IoT resources.

AWS IoT Policies

AWS IoT policies are JSON documents. They follow the same conventions as IAM policies. AWS IoT supports named policies so many identities can reference the same policy document. Named policies are versioned so they can be easily rolled back.
AWS IoT defines a set of policy actions that describe the operations and resources to which you can grant or deny access. For example:

- `iot:Connect` represents permission to connect to the AWS IoT message broker.
- `iot:Subscribe` represents permission to subscribe to an MQTT topic or topic filter.
- `iot:GetThingShadow` represents permission to get a device's shadow.

AWS IoT policies allow you to control access to the AWS IoT data plane. The AWS IoT data plane consists of operations that allow you to connect to the AWS IoT message broker, send and receive MQTT messages, and get or update a device's shadow. For more information, see AWS IoT Policy Actions (p. 133).

An AWS IoT policy is a JSON document that contains one or more policy statements. Each statement contains an Effect, an Action, and a Resource. The Effect specifies whether the action is allowed or denied. The Action specifies the action the policy is allowing or denying. The Resource specifies the resource or resources on which the action is allowed or denied. The following policy grants all devices permission to connect to the AWS IoT message broker, but restricts the device to publishing on a specific MQTT topic:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["iot:Publish"],
            "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/foo/bar"]
        },
        {
            "Effect": "Allow",
            "Action": ["iot:Connect"],
            "Resource": ["*"]
        }
    ]
}
```

**AWS IoT Policy Actions**

The following policy actions are defined by AWS IoT:

**MQTT Policy Actions**

`iot:Connect` represents the permission to connect to the AWS IoT message broker. The `iot:Connect` permission is checked every time a CONNECT request is sent to the broker. The message broker does not allow two clients with the same client ID to stay connected at the same time. After the second client connects, the broker detects this case and disconnects one of the clients. The `iot:Connect` permission can be used to ensure only authorized clients can connect using a specific client ID.

`iot:Publish` represents the permission to publish on an MQTT topic. This permission is checked every time a PUBLISH request is sent to the broker. This can be used to allow clients to publish to specific topic patterns.

**Note**

You must also grant `iot:Connect` permission to grant `iot:Publish` permission.

`iot:Receive` represents the permission to receive a message from AWS IoT. The `iot:Receive` permission is checked every time a message is delivered to a client. Because this permission is checked on every delivery, it can be used to revoke permissions to clients that are currently subscribed to a topic.
iot:Subscribe

Represents the permission to subscribe to a topic filter. This permission is checked every time a SUBSCRIBE request is sent to the broker. This can be used to allow clients to subscribe to topics that match specific topic patterns.

**Note**
You must also grant iot:Connect permission to grant iot:Subscribe permission.

**Shadow Policy Actions**

**iot:DeleteThingShadow**

Represents the permission to delete a device's shadow. The iot:DeleteThingShadow permission is checked every time a request is made to delete the shadow's contents.

**iot:GetThingShadow**

Represents the permission to retrieve a device's shadow. The iot:GetThingShadow permission is checked every time a request is made to retrieve the shadow's contents.

**iot:UpdateThingShadow**

Represents the permission to update a device's shadow. The iot:UpdateThingShadow permission is checked every time a request is made to update the shadow's contents.

**Note**
The job execution policy actions apply only for the HTTP TLS endpoint. If you use the MQTT endpoint, you must use MQTT policy actions defined in this topic.

**Job Executions Policy Actions**

**iot:DescribeJobExecution**

Represents the permission to retrieve a job execution for a given thing. The iot:DescribeJobExecution permission is checked every time a request is made to get the job execution.

**iot:GetPendingJobExecutions**

Represents the permission to retrieve the list of jobs that are not in a terminal status for a thing. The iot:GetPendingJobExecutions permission is checked every time a request is made to retrieve the list.

**iot:UpdateJobExecution**

Represents the permission to update a job execution. The iot:UpdateJobExecution permission is checked every time a request is made to update the state of a job execution.

**iot:StartNextPendingJobExecution**

Represents the permission to get and start the next pending job execution for a thing. (That is, to update a job execution with status QUEUED or IN_PROGRESS to IN_PROGRESS.) The iot:StartNextPendingJobExecution permission is checked every time a request is made to start the next pending job execution.

**Action Resources**

To specify a resource for an AWS IoT policy action, you must use the ARN of the resource. All resource ARNs are of the following form:
The following table shows the resource to specify for each action type:

<table>
<thead>
<tr>
<th>Action</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>iot:DeleteThingShadow</td>
<td>A thing ARN - arn:aws:iot:us-east-1:123456789012:thing/thingOne</td>
</tr>
<tr>
<td>iot:Connect</td>
<td>A client ID ARN - arn:aws:iot:us-east1:123456789012:client/myClientId</td>
</tr>
<tr>
<td>iot:UpdateThingShadow</td>
<td>A thing ARN - arn:aws:iot:us-east-1:123456789012:thing/thingOne</td>
</tr>
<tr>
<td>iot:GetThingShadow</td>
<td>A thing ARN - arn:aws:iot:us-east-1:123456789012:thing/thingOne</td>
</tr>
<tr>
<td>iot:DescribeJobExecution</td>
<td>A thing ARN - arn:aws:iot:us-east-1:123456789012:thing/thingOne</td>
</tr>
<tr>
<td>iot:GetPendingJobExecutions</td>
<td>A thing ARN - arn:aws:iot:us-east-1:123456789012:thing/thingOne</td>
</tr>
<tr>
<td>iot:StartNextPendingJobExecution</td>
<td>A thing ARN - arn:aws:iot:us-east-1:123456789012:thing/thingOne</td>
</tr>
</tbody>
</table>

**AWS IoT Policy Variables**

AWS IoT defines policy variables that can be used in AWS IoT policies within the resource or condition block. When a policy is evaluated, the policy variables are replaced by actual values. For example, if a device connected to the AWS IoT message broker with a client ID of "100-234-3456," the `iot:ClientId` policy variable would be replaced in the policy document by "100-234-3456." For more information about policy variables, see IAM Policy Variables and Multi-Value Conditions.

**Basic Policy Variables**

AWS IoT defines the following basic policy variables:

- `iot:ClientId`: The client ID used to connect to the AWS IoT message broker.
- `aws:SourceIp`: The IP address of the client connected to the AWS IoT message broker.

The following AWS IoT policy shows the use of policy variables:
In these examples, ${iot:ClientId} is replaced by the ID of the client connected to the AWS IoT message broker when the policy is evaluated. When you use policy variables like ${iot:ClientId}, you can inadvertently open access to unintended topics. For example, if you use a policy that uses ${iot:ClientId} to specify a topic filter:

```json
{
  "Effect": "Allow",
  "Action": ["iot:Subscribe"],
  "Resource": ["arn:aws:iot:us-east-1:123456789012:topicfilter/foo/${iot:ClientId}/bar"]
}
```

A client can connect using + as the client ID. This would allow the user to subscribe to any topic matching the topic filter `foo+/+bar`. To protect against such security gaps, use the `iot:Connect` policy action to control which client IDs are able to connect. For example, this policy allows only clients whose client ID is `clientid1` to connect:

```json
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["iot:Connect"],
    "Resource": ["arn:aws:iot:us-east-1:123456789012:client/clientid1"]
  }]
}
```

X.509 Certificate Policy Variables

X.509 certificate policy variables allow you to write AWS IoT policies that grant permissions based on X.509 certificate attributes. The following sections describe how you can use these certificate policy variables.

**Issuer Attributes**

The following AWS IoT policy variables allow you to allow or deny permissions based on certificate attributes set by the certificate issuer.

- `iot:Certificate.Issuer.DistinguishedNameQualifier`
Subject Attributes

The following AWS IoT policy variables allow you to grant or deny permissions based on certificate subject attributes set by the certificate issuer.

- `iot:Certificate.Subject.DistinguishedNameQualifier`
- `iot:Certificate.Subject.Country`
- `iot:Certificate.Subject.Organization`
- `iot:Certificate.Subject.OrganizationalUnit`
- `iot:Certificate.Subject.State`
- `iot:Certificate.Subject.CommonName`
- `iot:Certificate.Subject.SerialNumber`
- `iot:Certificate.Subject.Title`
- `iot:Certificate.Subject.Surname`
- `iot:Certificate.Subject.GivenName`
- `iot:Certificate.Subject.Initials`
- `iot:Certificate.Subject.Pseudonym`
- `iot:Certificate.Subject.GenerationQualifier`

X.509 certificates allow these attributes to contain one or more values. By default, the policy variables for each multi-value attribute return the first value. For example, the `Certificate.Subject.Country` attribute might contain a list of country names. When evaluated in a policy, `iot:Certificate.Subject.Country` is replaced by the first country name. You can request a specific attribute value using a one-based index. For example, `iot:Certificate.Subject.Country.1` is replaced by the second country name in the `Certificate.Subject.Country` attribute. If you specify an attribute value that does not exist (for example, if you ask for a third value when there are only two values assigned to the attribute), no substitution is made and authorization fails. You can use the `.List` suffix on the policy variable name to specify all values of the attribute. The following example policy allows any client to connect to AWS IoT, but restricts publishing rights to those clients with certificates whose `Certificate.Subject.Organization` attribute is set to "Example Corp" or "AnyCompany". This is done through the use of a "Condition" attribute that specifies a condition for the preceding action. The condition in this case is that the `Certificate.Subject.Organization` attribute of the certificate must include one of the listed values.

```
"Version": "2012-10-17",
"Statement":[
  {
    "Effect": "Allow",
    "Action": ["iot:Connect"],
    "Resource": [*]
  },
  {
    "Effect": "Allow",
    "Action": ["iot:Publish"],
    "Resource": [*],
    "Condition": {
      "ForAllValues:StringEquals": {
        "iot:Certificate.Subject.Organization.List": [
          "Example Corp",
          "AnyCompany"
        ]
      }
    }
  }
]}

**Issuer Alternate Name Attributes**

The following AWS IoT policy variables allow you to grant or deny permissions based on issuer alternate name attributes set by the certificate issuer.

- `iot:Certificate.Issuer.AlternativeName.RFC822Name`
- `iot:Certificate.Issuer.AlternativeName.DNSName`
- `iot:Certificate.Issuer.AlternativeName.DirectoryName`
- `iot:Certificate.Issuer.AlternativeName.IPAddress`

**Subject Alternate Name Attributes**

The following AWS IoT policy variables allow you to grant or deny permissions based on subject alternate name attributes set by the certificate issuer.

- `iot:Certificate.Subject.AlternativeName.RFC822Name`
- `iot:Certificate.Subject.AlternativeName.DNSName`
- `iot:Certificate.Subject.AlternativeName.DirectoryName`
- `iot:Certificate.Subject.AlternativeName.UniformResourceIdentifier`
- `iot:Certificate.Subject.AlternativeName.IPAddress`

**Other Attributes**

You can use `iot:Certificate.SerialNumber` to allow or deny access to AWS IoT resources based on the serial number of a certificate. The `iot:Certificate.AvailableKeys` policy variable contains the name of all certificate policy variables that contain values.
X.509 Certificate Policy Variable Limitations

The following limitations apply to X.509 certificate policy variables:

Wildcards

If wildcard characters are present in certificate attributes, the policy variable is not replaced by the certificate attribute value, leaving the \( \textit{\$\{policy-variable\}} \) text in the policy document. This might cause authorization failure.

Array fields

Certificate attributes that contain arrays are limited to five items. Additional items are ignored.

String length

All string values are limited to 1024 characters. If a certificate attribute contains a string longer than 1024 characters, the policy variable is not replaced by the certificate attribute value, leaving the \( \textit{\$\{policy-variable\}} \) in the policy document. This might cause authorization failure.

Thing Policy Variables

Thing policy variables allow you to write AWS IoT policies that grant or deny permissions based on thing properties like thing names, thing types, and thing attribute values. The thing name is obtained from the client ID in the MQTT \texttt{Connect} message sent when a thing connects to AWS IoT. The thing policy variables are replaced when a thing connects to AWS IoT over MQTT using TLS mutual authentication or MQTT over the WebSocket protocol using authenticated Amazon Cognito identities. Thing policy variables are also replaced when a certificate or authenticated Amazon Cognito identity is attached to a thing. You can use the \texttt{AttachThingPrincipal} API to attach certificates and authenticated Amazon Cognito identities to a thing.

The following thing policy variables are available:

- \texttt{iot:Connection.Thing.ThingName}
- \texttt{iot:Connection.Thing.ThingTypeName}
- \texttt{iot:Connection.Thing.Attributes[attributeName]}
- \texttt{iot:Connection.Thing.IsAttached}

\texttt{iot:Connection.Thing.ThingName}

This resolves to the name of the thing for which the policy is being evaluated. The thing name is set to the client ID of the MQTT/WebSocket connection. This policy variable is available only when connecting over MQTT or MQTT over the WebSocket protocol.

\texttt{iot:Connection.Thing.ThingTypeName}

This resolves to the thing type associated with the thing for which the policy is being evaluated. The thing name is set to the client ID of the MQTT/WebSocket connection. The thing type name is obtained by a call to the \texttt{DescribeThing} API. This policy variable is available only when connecting over MQTT or MQTT over the WebSocket protocol.

\texttt{iot:Connection.Thing.Attributes[attributeName]}

This resolves to the value of the specified attribute associated with the thing for which the policy is being evaluated. A thing can have up to 50 attributes. Each attribute is available as a policy variable: \texttt{iot:Connection.Thing.Attributes[attributeName]} where \texttt{attributeName} is the name of the attribute. The thing name is set to the client ID of the MQTT/WebSocket connection. This policy variable is only available when connecting over MQTT or MQTT over the WebSocket protocol.
iot:Connection.Thing.IsAttached

This resolves to true if the thing for which the policy is being evaluated has a certificate or Amazon Cognito identity attached.

Example Policies

AWS IoT policies are specified in a JSON document. These are the components of an AWS IoT policy:

Version

Must be set to "2012-10-17".

Effect

Must be set to "Allow" or "Deny".

Action

Must be set to "iot:operation-name" where operation-name is one of the following:

"iot:Connect": Connect to AWS IoT
"iot:Receive": Receive messages from AWS IoT
"iot:Publish": MQTT publish.
"iot:Subscribe": MQTT subscribe.
"iot:UpdateThingShadow": Update a device's shadow.
"iot:GetThingShadow": Retrieve a device's shadow.
"iot:DeleteThingShadow": Delete a device's shadow.

Resource

Must be set to one of the following:


Connect Policy Examples

The following policy allows a set of client IDs to connect:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["iot:Connect"],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:client/clientid2",
                "arn:aws:iot:us-east-1:123456789012:client/clientid3"
            ]
        },
        {
            "Effect": "Allow",
            "Action": ["iot:Connect"],
            "Resource": [
            ]
        }
    ]
}
```
"Effect": "Allow",
"Action": [
  "iot:Publish",
  "iot:Subscribe",
  "iot:Receive"
],
"Resource": ["*"]
}
}

The following policy prevents a set of client IDs from connecting:

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "iot:Connect"
      ],
      "Resource": [
        "arn:aws:iot:us-east-1:123456789012:client/clientid2"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Connect"
      ],
      "Resource": ["*"]
    }
  ]
}

The following policy allows the certificate holder using any client ID to subscribe to topic filter foo/*:

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Connect"
      ],
      "Resource": ["*"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
      "Resource": ["arn:aws:iot:us-east-1:123456789012:topicfilter/foo/*"]
    }
  ]
}
Publish/Subscribe Policy Examples

The policy you use depends on how you are connecting to AWS IoT. You can connect to AWS IoT using an MQTT client, HTTP, or WebSocket. When you connect with an MQTT client, you are authenticating with an X.509 certificate. When you connect over HTTP or the WebSocket protocol, you are authenticating with Signature Version 4 and Amazon Cognito.

Policies for MQTT Clients

When you specify topic filters in AWS IoT policies for MQTT clients, MQTT wildcard characters "+" and "#" are treated as literal characters. Their use might result in unexpected behavior. For example, the following policy allows a client to subscribe to the topic filter `foo/+/bar` only:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Connect"
      ],
      "Resource": [
        "*"
      ],
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
      "Resource": [
        "arn:aws:iot:us-east-1:123456789012:topicfilter/foo/+/bar"
      ]
    }
  ]
}
```

**Note**

The MQTT wildcard character '+' is not treated as a wildcard within a policy. Attempts to subscribe to topic filters that match the pattern `foo/+/bar` like `foo/baz/bar` or `foo/goo/bar` fails and causes the client to disconnect.

You can use "*" as a wildcard in the resource attribute of the policy. For example, the following policy allows the certificate holder to publish to all topics and subscribe to all topic filters in the AWS account:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```
The following policy allows the certificate holder to publish to all topics in the AWS account:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish",
        "iot:Connect"
      ],
      "Resource": [
        "*
      ]
    }
  ]
}
```

You can also use the "*" wildcard at the end of a topic filter. For example, the following policy allows the certificate holder to subscribe to a topic filter matching the pattern `foo/bar/*`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Connect"
      ],
      "Resource": [
        "*
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
      "Resource": [
        "arn:aws:iot:us-east-1:123456789012:topicfilter/foo/bar/*"
      ]
    }
  ]
}
```

The following policy allows the certificate holder to publish to the `foo/bar` and `foo/baz` topics:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Connect"
      ],
      "Resource": [
        "*
      ]
    }
  ]
}
```
The following policy prevents the certificate holder from publishing to the `foo/bar` topic:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [ "iot:Publish" ],
    }
  ]
}
```

The following policy allows the certificate holder to publish on topic `foo` and prevents the certificate holder from publishing to topic `bar`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "iot:Publish" ],
    }
  ]
}
```
The following policy allows the certificate holder to subscribe to topic filter `foo/bar`:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "iot:Connect"
         ],
         "Resource": ["*"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "iot:Subscribe"
         ],
         "Resource": ["arn:aws:iot:us-east-1:123456789012:topicfilter/foo/bar"
         ]
      }
   ]
}
```

The following policy allows the certificate holder to publish on the `arn:aws:iot:us-east-1:123456789012:topic/iotmonitor/provisioning/8050373158915119971` topic and allows the certificate holder to subscribe to the topic filter `arn:aws:iot:us-east-1:123456789012:topicfilter/iotmonitor/provisioning/8050373158915119971`:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "iot:Connect"
         ],
         "Resource": ["*"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "iot:Publish",
            "iot:Receive"
         ],
         "Resource": ["arn:aws:iot:us-east-1:123456789012:topicfilter/iotmonitor/provisioning/8050373158915119971"
         ]
      }
   ]
}
```
"arn:aws:iot:us-east-1:123456789012:topic/iotmonitor/provisioning/8050373158915119971"
],
},
{
"Effect": "Allow",
"Action": [
"iot:Subscribe"
],
"Resource": [
"arn:aws:iot:us-east-1:123456789012:topicfilter/iotmonitor/provisioning/8050373158915119971"
]
}
}

Policies for HTTP and WebSocket Clients

For the following operations, AWS IoT uses AWS IoT policies attached to Amazon Cognito identities (through the AttachPolicy API) to scope down the permissions attached to the Amazon Cognito identity pool with authenticated identities. That means an Amazon Cognito identity needs permission from the IAM role policy attached to the pool and the AWS IoT policy attached to the Amazon Cognito identity through the AWS IoT AttachPolicy API.

- iot:Connect
- iot:Publish
- iot:Subscribe
- iot:Receive
- iot:GetThingShadow
- iot:UpdateThingShadow
- iot:DeleteThingShadow

**Note**

For other AWS IoT operations or for unauthenticated identities, AWS IoT does not scope down the permissions attached to the Amazon Cognito identity pool role. For both authenticated and unauthenticated identities, this is the most permissive policy that we recommend attaching to the Amazon Cognito pool role.

To allow unauthenticated Amazon Cognito identities to publish messages over HTTP on any topic, attach the following policy to the Amazon Cognito identity pool role:

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "iot:Connect",
         "iot:Publish",
         "iot:Subscribe",
         "iot:Receive",
         "iot:GetThingShadow",
         "iot:UpdateThingShadow",
         "iot:DeleteThingShadow"
      ],
      "Resource": ["*""
   }
   ]
}
```
To allow unauthenticated Amazon Cognito identities to publish MQTT messages over HTTP on any topic in your account, attach the following policy to the Amazon Cognito identity pool role:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["iot:Publish"],
        "Resource": ["*"]
    }
}
```

**Note**

This example is for illustration only. Unless your service absolutely requires it, we recommend the use of a more restrictive policy, one that does not allow unauthenticated Amazon Cognito identities to publish on any topic.

To allow unauthenticated Amazon Cognito identities to publish MQTT messages over HTTP on topic1 in your account, attach the following policy to your Amazon Cognito identity pool role:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["iot:Publish"],
        "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/topic1"]
    }
}
```

For an authenticated Amazon Cognito identity to publish MQTT messages over HTTP on topic1 in your AWS account, you must specify two policies, as outlined here. The first policy must be attached to an Amazon Cognito identity pool role. It allows identities from that pool to make a publish call. The second policy must be attached to an Amazon Cognito user using the AWS IoT AttachPolicy API. It allows the specified Amazon Cognito user access to the topic1 topic.

**Amazon Cognito identity pool policy:**

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["iot:Publish"],
        "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/topic1"]
    }
}
```

**Amazon Cognito user policy:**

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["iot:Publish"],
        "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/topic1"]
    }
}
```

Similarly, the following example policy allows the Amazon Cognito user to publish MQTT messages over HTTP on the topic1 and topic2 topics. Two policies are required. The first policy gives the Amazon
Cognito identity pool role the ability to make the publish call. The second policy gives the Amazon Cognito user access to the topic1 and topic2 topics.

Amazon Cognito identity pool policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["iot:Publish"],
    "Resource": ["*"]
  }]
}
```

Amazon Cognito user policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["iot:Publish"],
    "Resource": [
      "arn:aws:iot:us-east-1:123456789012:topic/topic1",
      "arn:aws:iot:us-east-1:123456789012:topic/topic2"
    ]
  }]
}
```

The following policies allow multiple Amazon Cognito users to publish to a topic. Two policies per Amazon Cognito identity are required. The first policy gives the Amazon Cognito identity pool role the ability to make the publish call. The second and third policies give the Amazon Cognito users access to the topics topic1 and topic2, respectively.

Amazon Cognito identity pool policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["iot:Publish"],
    "Resource": ["*"]
  }]
}
```

Amazon Cognito user1 policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["iot:Publish"],
    "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/topic1"]
  }]
}
```

Amazon Cognito user2 policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["iot:Publish"],
    "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/topic2"]
  }]
}
```
Receive Policy Examples

The following policy prevents the certificate holder using any client ID from receiving messages from a topic:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": ["iot:Receive"],
      },
      {
         "Effect": "Allow",
         "Action": ["iot:*"],
         "Resource": ["*"]
      }
   ]
}
```

The following policy allows the certificate holder using any client ID to subscribe and receive messages on one topic:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": ["iot:Connect"],
         "Resource": ["*"]
      },
      {
         "Effect": "Allow",
         "Action": ["iot:Subscribe"],
         "Resource": ["arn:aws:iot:us-east-1:123456789012:topicfilter/foo/bar"]
      },
      {
         "Effect": "Allow",
         "Action": ["iot:Receive"],
         "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/foo/bar"]
      }
   ]
}
```
Certificate Policy Examples

The following policy allows a device to publish on a topic whose name is equal to the certificateId of the certificate with which the device authenticated itself:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["iot:Publish"],
        },
        {
            "Effect": "Allow",
            "Action": ["iot:Connect"],
            "Resource": ["*"]
        }
    ]
}
```

The following policy allows a device to publish on a topic whose name is equal to the subject's common name field of the certificate with which the device authenticated itself:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["iot:Publish"],
        },
        {
            "Effect": "Allow",
            "Action": ["iot:Connect"],
            "Resource": ["*"]
        }
    ]
}
```

The following policy allows a device to publish on a topic that is prefixed with "admin/" when the certificate used to authenticate the device has its Subject.CommonName.2 field set to "Administrator":

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["iot:Connect"],
            "Resource": ["*"]
        },
        {
            "Effect": "Allow",
            "Action": ["iot:Publish"],
            "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/admin/*"],
            "Condition": {
                "StringEquals": {
                    "iot:Certificate.Subject.CommonName.2": "Administrator"
                }
            }
        }
    ]
}
```
The following policy allows a device to publish on a topic that is prefixed with "admin/" when the certificate used to authenticate the device has any one of its Subject.Common fields set to "Administrator":

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["iot:Connect"],
        "Resource": ["*"]
    }, {
        "Effect": "Allow",
        "Action": ["iot:Publish"],
        "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/admin/**"],
        "Condition": {
            "ForAnyValue:StringEquals": {
                "iot:Certificate.Subject.CommonName.List": "Administrator"
            }
        }
    }]
}
```

**Thing Policy Examples**

The following policy allows a thing to publish on a specific topic that contains the thing type name and thing name:

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["iot:Publish"],
        "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/${iot:Connection.Thing.ThingTypeName}/${iot:Connection.Thing.ThingName}"
    }]
}
```

The following policy allows the device to connect if the certificate used to authenticate with AWS IoT is attached to the thing for which the policy is being evaluated.

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["iot:Connect"],
        "Resource": ["*"],
        "Condition": {
            "Bool": {
                "iot:Connection.Thing.IsAttached": ["true"
            }
        }
    }]
}
```

The following policy allows a device to publish on a set of topics ("/foo/bar" and "/foo/baz") if:
The thing associated with the device has an attribute called "Manufacturer" with a value of "foo," "bar," or "baz."

The thing associated with the device exists in the registry and is attached to the certificate used to connect to AWS IoT.

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["iot:Publish"],
                      "arn:aws:iot:us-east-1:123456789012:topic/foo/baz"],
        "Condition": {
            "ForAnyValue:StringLike": {
                "iot:Connection.Thing.Attributes[Manufacturer]": [
                    "foo",
                    "bar",
                    "baz"
                ]
            }
        }
    }]
}
```

The following policy allows a device to publish to a topic if:

- The topic is composed of the thing type name, a '/', and the thing name.
- The thing exists in the registry.
- The thing is attached to the certificate used to connect to AWS IoT.

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["iot:Publish"],
        "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/${iot:Connection.Thing.ThingTypeName}/${iot:Connection.Thing.ThingName}"
                      ]
    }]
}
```

The following policy allows a device to publish only on its own shadow topic, if the corresponding thing exists in the registry.

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["iot:Publish"],
                      ]
    }]
}
```
IAM IoT Policies

AWS Identity and Access Management defines a policy action for each operation defined by AWS IoT, including control plane and data plane APIs.

AWS IoT API Permissions

The following table lists the AWS IoT API, the IAM permissions required, and the resource the API manipulates.

<table>
<thead>
<tr>
<th>API</th>
<th>Required permission (policy actions)</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>The AWS account specified in the ARN must be the account to which the certificate is being transferred.</td>
</tr>
<tr>
<td>AddLoggingRole</td>
<td>iot:AddLoggingRole</td>
<td>none</td>
</tr>
<tr>
<td>AddThingToThingGroup</td>
<td>iot:AddThingToThingGroup</td>
<td>arn:aws:iot:region:account-id:thinggroup/thing-group-name</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td>arn:aws:iot:region:account-id:thing/thing-name</td>
</tr>
<tr>
<td>AssociateTargetsWithJob</td>
<td>iot:AssociateTargetsWithJob</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td>arn:aws:iot:region:account-id:cert/cert-id</td>
</tr>
<tr>
<td>AttachThingPrincipal</td>
<td>iot:AttachThingPrincipal</td>
<td>arn:aws:iot:region:account-id:cert/cert-id</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>The AWS account specified in the ARN must be the account to which the certificate is being transferred.</td>
</tr>
<tr>
<td>CreateAuthorizer</td>
<td>iot:CreateAuthorizer</td>
<td>arn:aws:iot:region:account-id:authorizer/authorizer-function-name</td>
</tr>
</tbody>
</table>
### IAM IoT Policies

<table>
<thead>
<tr>
<th>API</th>
<th>Required permission (policy actions)</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateKeysAndCertificate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CreatePolicy</td>
<td>iot:CreatePolicy</td>
<td>*</td>
</tr>
<tr>
<td>CreatePolicyVersion</td>
<td>iot:CreatePolicyVersion</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> This must be an AWS IoT policy, not an IAM policy.</td>
</tr>
<tr>
<td>CreateRoleAlias</td>
<td>iot:CreateRoleAlias</td>
<td>(parameter: roleAlias)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>arn:aws:iot:region:account-id:rolealias/role-alias-name</td>
</tr>
<tr>
<td>CreateThing</td>
<td>iot:CreateThing</td>
<td>arn:aws:iot:region:account-id:thing/thing-name</td>
</tr>
<tr>
<td>CreateThingGroup</td>
<td>iot:CreateThingGroup</td>
<td>arn:aws:iot:region:account-id:thinggroup/thing-group-name for group being created and for parent group, if used</td>
</tr>
<tr>
<td>CreateThingType</td>
<td>iot:CreateThingType</td>
<td>arn:aws:iot:region:account-id:thingtype/thing-type-name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>arn:aws:iot:region:account-id:thing/thing-name</td>
</tr>
<tr>
<td>DeleteLoggingLevel</td>
<td>iot:DeleteLoggingLevel</td>
<td>arn:aws:iot:region:account-id:thinggroup/thing-group-name</td>
</tr>
<tr>
<td>DeleteLoggingRole</td>
<td>iot:DeleteLoggingRole</td>
<td>none</td>
</tr>
<tr>
<td>DeleteRegistrationCode</td>
<td>iot:DeleteRegistrationCode</td>
<td></td>
</tr>
<tr>
<td>DeleteThing</td>
<td>iot:DeleteThing</td>
<td>arn:aws:iot:region:account-id:thing/thing-name</td>
</tr>
<tr>
<td>DeleteThingGroup</td>
<td>iot:DeleteThingGroup</td>
<td>arn:aws:iot:region:account-id:thinggroup/thing-group-name</td>
</tr>
<tr>
<td>API</td>
<td>Required permission (policy actions)</td>
<td>Resources</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DeleteThingType</td>
<td>iot:DeleteThingType</td>
<td>arn:aws:iot:region:account-id:thingtype/thing-type-name</td>
</tr>
<tr>
<td>DeleteV2LoggingLevel</td>
<td>iot:DeleteV2LoggingLevel</td>
<td>arn:aws:iot:region:account-id:thinggroup/thing-group-name</td>
</tr>
<tr>
<td>DeprecateThingType</td>
<td>iot:DeprecateThingType</td>
<td>arn:aws:iot:region:account-id:thingtype/thing-type-name</td>
</tr>
<tr>
<td>DescribeIndex</td>
<td>iot:DescribeIndex</td>
<td>arn:aws:iot:region:account-id:index/index-name</td>
</tr>
<tr>
<td>DescribeRoleAlias</td>
<td>iot:DescribeRoleAlias</td>
<td>arn:aws:iot:region:account-id:rolealias/role-alias-name</td>
</tr>
<tr>
<td>DescribeThing</td>
<td>iot:DescribeThing</td>
<td>arn:aws:iot:region:account-id:thing/thing-name</td>
</tr>
<tr>
<td>DescribeThingGroup</td>
<td>iot:DescribeThingGroup</td>
<td>arn:aws:iot:region:account-id:thinggroup/thing-group-name</td>
</tr>
<tr>
<td>DescribeThingRegistrationTask</td>
<td>iot:DescribeThingRegistrationTask</td>
<td>arn:aws:iot:region:account-id:thingtype/thing-type-name</td>
</tr>
<tr>
<td>DetachThingPrincipal</td>
<td>iot:DetachThingPrincipal</td>
<td>arn:aws:iot:region:account-id:cert/cert-id</td>
</tr>
<tr>
<td>API</td>
<td>Required permission (policy actions)</td>
<td>Resources</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>GetIndexingConfiguration</td>
<td>iot:GetIndexingConfiguration</td>
<td></td>
</tr>
<tr>
<td>GetLoggingOptions</td>
<td>iot:GetLoggingOptions</td>
<td></td>
</tr>
<tr>
<td>GetLoggingRole</td>
<td>iot:GetLoggingRole</td>
<td>none</td>
</tr>
<tr>
<td>GetRegistrationCode</td>
<td>iot:GetRegistrationCode</td>
<td></td>
</tr>
<tr>
<td>GetV2LoggingOptions</td>
<td>iot:GetV2LoggingOptions</td>
<td></td>
</tr>
<tr>
<td>ListAuthorizers</td>
<td>iot:ListAuthorizers</td>
<td>none</td>
</tr>
<tr>
<td>ListCACertificates</td>
<td>iot:ListCACertificates</td>
<td>*</td>
</tr>
<tr>
<td>ListCertificates</td>
<td>iot:ListCertificates</td>
<td>*</td>
</tr>
<tr>
<td>ListCertificatesByCA</td>
<td>iot:ListCertificatesByCA</td>
<td></td>
</tr>
<tr>
<td>ListIndices</td>
<td>iot:ListIndices</td>
<td>none</td>
</tr>
<tr>
<td>ListJobExecutionsForJob</td>
<td>iot:ListJobExecutionsForJob</td>
<td></td>
</tr>
<tr>
<td>ListJobExecutionsForThing</td>
<td>iot:ListJobExecutionsForThing</td>
<td></td>
</tr>
<tr>
<td>ListJobs</td>
<td>iot:ListJobs</td>
<td>arn:aws:iot:region:account-id:thinggroup/thing-group-name if thingGroupName parameter used</td>
</tr>
<tr>
<td>ListLoggingLevels</td>
<td>iot:ListLoggingLevels</td>
<td>none</td>
</tr>
<tr>
<td>ListOutgoingCertificates</td>
<td>iot:ListOutgoingCertificates</td>
<td></td>
</tr>
<tr>
<td>ListPolicies</td>
<td>iot:ListPolicies</td>
<td>*</td>
</tr>
<tr>
<td>API</td>
<td>Required permission (policy actions)</td>
<td>Resources</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ListRoleAliases</td>
<td>iot:ListRoleAliases</td>
<td>none</td>
</tr>
<tr>
<td>ListThingGroups</td>
<td>iot:ListThingGroups</td>
<td>none</td>
</tr>
<tr>
<td>ListThingGroupsForThingGroup</td>
<td>iot:ListThingGroupsForThingGroup</td>
<td>arn:aws:iot:region:account-id:thinggroup/thing-group-name</td>
</tr>
<tr>
<td>ListThingRegistrationTasks</td>
<td>iot:ListThingRegistrationTasks</td>
<td></td>
</tr>
<tr>
<td>ListThingRegistrationTaskReports</td>
<td>iot:ListThingRegistrationTaskReports</td>
<td></td>
</tr>
<tr>
<td>ListThingTypes</td>
<td>iot:ListThingTypes</td>
<td>*</td>
</tr>
<tr>
<td>ListThings</td>
<td>iot:ListThings</td>
<td>*</td>
</tr>
<tr>
<td>ListThingsInThingGroup</td>
<td>iot:ListThingsInThingGroup</td>
<td>arn:aws:iot:region:account-id:thinggroup/thing-group-name</td>
</tr>
<tr>
<td>ListTopicRules</td>
<td>iot:ListTopicRules</td>
<td>*</td>
</tr>
<tr>
<td>ListV2LoggingLevels</td>
<td>iot:ListV2LoggingLevels</td>
<td>none</td>
</tr>
<tr>
<td>RegisterCACertificate</td>
<td>iot:RegisterCACertificate</td>
<td></td>
</tr>
<tr>
<td>RegisterCertificate</td>
<td>iot:RegisterCertificate</td>
<td></td>
</tr>
<tr>
<td>RegisterThing</td>
<td>iot:RegisterThing</td>
<td>none</td>
</tr>
<tr>
<td>RemoveThingFromThingGroup</td>
<td>iot:RemoveThingFromThingGroup</td>
<td>arn:aws:iot:region:account-id:thinggroup/thing-group-name</td>
</tr>
<tr>
<td>SearchIndex</td>
<td>iot:SearchIndex</td>
<td>arn:aws:iot:region:account-id:index/index-id</td>
</tr>
<tr>
<td>SetLoggingLevel</td>
<td>iot:SetLoggingLevel</td>
<td>none</td>
</tr>
<tr>
<td>SetLoggingOptions</td>
<td>iot:SetLoggingOptions</td>
<td>arn:aws:iot:region:account-id:role/role-name</td>
</tr>
<tr>
<td>SetV2LoggingLevel</td>
<td>iot:SetV2LoggingLevel</td>
<td>arn:aws:iot:region:account-id:thinggroup/thing-group-name</td>
</tr>
<tr>
<td>SetV2LoggingOptions</td>
<td>iot:SetV2LoggingOptions</td>
<td>arn:aws:iot:region:account-id:role/role-name</td>
</tr>
<tr>
<td>StartThingRegistrationTask</td>
<td>iot:StartThingRegistrationTask</td>
<td></td>
</tr>
</tbody>
</table>
IAM IoT Policies

AWS IoT provides a set of IAM policy templates you can either use as-is or as a starting point for creating custom IAM policies. These templates allow access to configuration and data operations. Configuration operations allow you to create things, certificates, policies, and rules. Data operations send data over MQTT or HTTP protocols. The following table describes these templates.

<table>
<thead>
<tr>
<th>Policy Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWSIoTLogging</td>
<td>Allows the associated identity to configure CloudWatch logging. This policy is attached to your CloudWatch logging role.</td>
</tr>
<tr>
<td>AWSIoTConfigAccess</td>
<td>Allows the associated identity access to all AWS IoT configuration operations. This policy can affect data processing and storage.</td>
</tr>
<tr>
<td>AWSIoTConfigReadOnlyAccess</td>
<td>Allows the associated identity to call read-only configuration operations.</td>
</tr>
<tr>
<td>AWSIoTDataAccess</td>
<td>Allows the associated identity full access to all AWS IoT data operations. Data operations send data over MQTT or HTTP protocols.</td>
</tr>
</tbody>
</table>

IAM Policy Templates
Authorizing Direct Calls to AWS Services

Devices can use X.509 certificates to connect to AWS IoT using TLS mutual authentication protocols. Other AWS services do not support certificate-based authentication, but they can be called using AWS credentials in AWS Signature Version 4 format. The Signature Version 4 algorithm normally requires the caller to have an access key ID and a secret access key. AWS IoT has a credentials provider that allows you to use the built-in X.509 certificate as the unique device identity to authenticate AWS requests. This eliminates the need to store an access key ID and a secret access key on your device.

The credentials provider authenticates a caller using an X.509 certificate and issues a temporary, limited-privilege security token. The token can be used to sign and authenticate any AWS request. This way of authenticating your AWS requests requires you to create and configure an AWS Identity and Access Management (IAM) role and attach appropriate IAM policies to the role so that the credentials provider can assume the role on your behalf.

**Note**

The credentials provider feature is not available in the China (Beijing) Region.

The following diagram illustrates the credentials provider workflow.
1. The AWS IoT device makes an HTTPS request to the credentials provider for a security token. The request includes the device X.509 certificate for authentication.

2. The credentials provider forwards the request to the AWS IoT authentication and authorization module to validate the certificate and verify that it has permission to request the security token.

3. If the certificate is valid and has permission to request a security token, the AWS IoT authentication and authorization module returns success. Otherwise, it sends an exception to the device.

4. After successfully validating the certificate, the credentials provider invokes the AWS Security Token Service (AWS STS) to assume the IAM role that you created for it.

5. AWS STS returns a temporary, limited-privilege security token to the credentials provider.

6. The credentials provider returns the security token to the device.

7. The device uses the security token to sign an AWS request with AWS Signature Version 4.

8. The requested service invokes IAM to validate the signature and authorize the request against access policies attached to the IAM role that you created for the credentials provider.

9. If IAM validates the signature successfully and authorizes the request, the request succeeds. Otherwise, IAM sends an exception.

The following section describes how to use a certificate to get a security token. It assumes that you have already registered a device and created and activated your own certificate for it.

**How to Use a Certificate to Get a Security Token**

1. Configure the IAM role that the credentials provider assumes on behalf of your device. Attach the following trust policy to the role.
For each AWS service that you want to call, attach an access policy to the role. The credentials provider supports the following policy variables:

- credentials-iot:ThingName
- credentials-iot:ThingTypeName
- credentials-iot:AwsCertificateId

When the device provides the thing name in its request to an AWS service, the credentials provider adds credentials-iot:ThingName and credentials-iot:ThingTypeName as context variables to the security token. The credentials provider provides credentials-iot:AwsCertificateId as a context variable even if the device doesn't provide the thing name in the request. You pass the thing name as the value of the x-amzn-iot-thingname HTTP request header.

These three variables work for IAM policies only, not AWS IoT policies.

2. Make sure that the user who performs the next step (creating a role alias) has permission to pass this newly created role to AWS IoT. The following policy gives both iam:GetRole and iam:PassRole permissions to an AWS user. The iam:GetRole permission enables the user to get information about the role that you've just created. The iam:PassRole permission enables the user to pass the role to another AWS service.

3. Create an AWS IoT role alias. The device that is going to make direct calls to AWS services must know which role ARN to use when connecting to AWS IoT. Hard-coding the role ARN is not a good solution because it requires you to update the device whenever the role ARN changes. A better solution is to use the CreateRoleAlias API to create a role alias that points to the role ARN. If the role ARN changes, you simply update the role alias. No change is required on the device. This API takes the following parameters:
4. Attach a policy to the device certificate. The policy attached to the device certificate must
grant the device permission to assume the role. You do this by granting permission for the
`iot:AssumeRoleWithCertificate` action to the role alias, as in the following example.

```json
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "iot:AssumeRoleWithCertificate",
        "Resource": "arn:aws:iot:your region:your aws account id:rolealias/your role alias"
    }
}
```

5. Make an HTTPS request to the credentials provider to get a security token. Supply the following
information.

- **Certificate**: Because this is an HTTP request over TLS mutual authentication, you have to provide
  the certificate and the corresponding private key to your client while making the request. Use the
  same certificate and private key that you used when you registered your certificate with AWS IoT.

  To make sure your device is communicating with AWS IoT (and not a service impersonating it),
  copy the Amazon root CA 1 for RSA and the VeriSign Class 3 Public Primary G5 root CA certificate
to your device.

- **RoleAlias**: The name of the role alias that you created for the credentials provider.

- **ThingName**: The thing name that you created when you registered your AWS IoT thing. This is
  passed as the value of the `x-amzn-iot-thingname` HTTP header. This value is required only if
  you are using thing attributes as policy variables in AWS IoT or IAM policies.

Run the following command in the AWS CLI to obtain the credentials provider endpoint for your
AWS account. For more information about this API, see `DescribeEndpoint`.

```
aws iot describe-endpoint --endpoint-type iot:CredentialProvider
```

The following JSON object is sample output of the `describe-endpoint` command. It contains the
endpointAddress that you use to request a security token.

```json
{
}
```
Use the endpoint to make an HTTPS request to the credentials provider to return a security token. The following sample uses curl but you can use any HTTP client.

```
curl --cert your certificate --key your device certificate key pair -H "x-amzn-iot-thingname: your thing name" --cacert AmazonRootCA1.pem https://your endpoint/role-aliases/your role alias/credentials
```

This command returns a security token object that contains an accessKeyId, a secretAccessKey, a sessionToken, and an expiration. The following JSON object is sample output of the curl command.

```
{"credentials":{"accessKeyId":"access key","secretAccessKey":"secret access key","sessionToken":"session token","expiration":"2018-01-18T09:18:06Z"}}
```

You can then use the accessKeyId, secretAccessKey, and sessionToken values to sign requests to AWS services. For an end-to-end demonstration of a specific use case, see How to Eliminate the Need for Hard-Coded AWS Credentials in Devices by Using the AWS IoT Credential Provider.

---

**Cross Account Access**

AWS IoT allows you to enable a principal to publish or subscribe to a topic that is defined in an AWS account not owned by the principal. You configure cross account access by creating an IAM policy and IAM role and then attaching the policy to the role.

First, create an IAM policy just like you would for other users and certificates in your AWS account. For example, the following policy grants permissions to connect and publish to the /foo/bar topic.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Connect"
      ],
      "Resource": [
        "*
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish"
      ],
      "Resource": [
        "arn:aws:iot:us-east-1:123456789012:topic/foo/bar"
      ]
    }
  ]
}
```
Next, follow the steps in Creating a Role for an IAM User. Enter the AWS account ID of the AWS account with which you want to share access. Then, in the final step, attach the policy you just created to the role. If, at a later time, you need to modify the AWS account ID to which you are granting access, you can use the following trust policy format to do so.

```json
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam:us-east-1:111111111111:user/MyUser"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

**Transport Security**

The AWS IoT message broker and Device Shadow service encrypt all communication with TLS version 1.2. TLS is used to ensure the confidentiality of the application protocols (MQTT, HTTP) supported by AWS IoT. TLS is available in a number of programming languages and operating systems.

For MQTT, TLS encrypts the connection between the device and the broker. TLS client authentication is used by AWS IoT to identify devices. For HTTP, TLS encrypts the connection between the device and the broker. Authentication is delegated to AWS Signature Version 4.

**TLS Cipher Suite Support**

AWS IoT supports the following cipher suites:

- ECDHE-ECDSA-AES128-GCM-SHA256 (recommended)
- ECDHE-RSA-AES128-GCM-SHA256 (recommended)
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA
- ECDHE-ECDSA-AES256-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES256-GCM-SHA384
- AES256-SHA256
- AES256-SHA
Message Broker for AWS IoT

The AWS IoT message broker is a publish/subscribe broker service that enables the sending and receiving of messages to and from AWS IoT. When communicating with AWS IoT, a client sends a message addressed to a topic like Sensor/temp/room1. The message broker, in turn, sends the message to all clients that have registered to receive messages for that topic. The act of sending the message is referred to as publishing. The act of registering to receive messages for a topic filter is referred to as subscribing.

The topic namespace is isolated for each AWS account and region pair. For example, the Sensor/temp/room1 topic for an AWS account is independent from the Sensor/temp/room1 topic for another AWS account. This is true of regions, too. The Sensor/temp/room1 topic in the same AWS account in us-east-1 is independent from the same topic in us-east-2. AWS IoT does not support sending and receiving messages across AWS accounts and regions.

The message broker maintains a list of all client sessions and the subscriptions for each session. When a message is published on a topic, the broker checks for sessions with subscriptions that map to the topic. The broker then forwards the publish message to all sessions that have a currently connected client.

Protocols

The message broker supports the use of the MQTT protocol to publish and subscribe and the HTTPS protocol to publish. Both protocols are supported through IP version 4 and IP version 6. The message broker also supports MQTT over the WebSocket protocol.

Protocol/Port Mappings

The following table shows each protocol supported by AWS IoT, the authentication method, and port used for each protocol.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Authentication</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>MQTT</td>
<td>Client Certificate</td>
<td>8883, 443</td>
</tr>
<tr>
<td>HTTP</td>
<td>Client Certificate</td>
<td>8443</td>
</tr>
<tr>
<td>HTTP</td>
<td>SigV4</td>
<td>443</td>
</tr>
<tr>
<td>MQTT + WebSocket</td>
<td>SigV4</td>
<td>443</td>
</tr>
</tbody>
</table>

†Clients wishing to connect using MQTT with X.509 Client Certificate authentication on port 443 must implement the Application Layer Protocol Negotiation (ALPN) TLS extension and pass x-amzn-mqtt-ca as the ProtocolName in the ProtocolNameList. Note that ALPN is not required to open connections using MQTT with X.509 Client Certificate authentication on port 8883.

MQTT

MQTT is a widely adopted lightweight messaging protocol designed for constrained devices. For more information, see MQTT.

Although the AWS IoT message broker implementation is based on MQTT version 3.1.1, it deviates from the specification as follows:
• In AWS IoT, subscribing to a topic with Quality of Service (QoS) 0 means a message will be delivered zero or more times. A message might be delivered more than once. Messages delivered more than once might be sent with a different packet ID. In these cases, the DUP flag is not set.

• AWS IoT does not support publishing and subscribing with QoS 2. The AWS IoT message broker does not send a PUBACK or SUBACK when QoS 2 is requested.

• The QoS levels for publishing and subscribing to a topic have no relation to each other. One client can subscribe to a topic using QoS 1 while another client can publish to the same topic using QoS 0.

• When responding to a connection request, the message broker sends a CONNACK message. This message contains a flag to indicate if the connection is resuming a previous session. The value of this flag might be incorrect if two MQTT clients connect with the same client ID simultaneously.

• When a client subscribes to a topic, there might be a delay between the time the message broker sends a SUBACK and the time the client starts receiving new matching messages.

• The MQTT specification provides a provision for the publisher to request that the broker retain the last message sent to a topic and send it to all future topic subscribers. AWS IoT does not support retained messages. If a request is made to retain messages, the connection is disconnected.

• The message broker uses the client ID to identify each client. The client ID is passed in from the client to the message broker as part of the MQTT payload. Two clients with the same client ID are not allowed to be connected concurrently to the message broker. When a client connects to the message broker using a client ID that another client is using, a CONNACK message will be sent to both clients and the currently connected client will be disconnected.

• The message broker does not support persistent sessions (connections made with the cleanSession flag set to false). The AWS IoT message broker assumes all sessions are clean sessions and messages are not stored across sessions. If an MQTT client attempts to connect to the AWS IoT message broker with the cleanSession set to false, the client will be disconnected.

• On rare occasions, the message broker might resend the same logical PUBLISH message with a different packet ID.

• The message broker does not guarantee the order in which messages and ACK are received.

**HTTP**

The message broker supports clients connecting with the HTTP protocol using a REST API. Clients can publish by sending a POST message to `<AWS IoT Endpoint>/<url_encoded_topic_name>?qos=1`.

For example, you can use curl to emulate a button press. If you followed the tutorial in Getting Started with AWS IoT (p. 5), rather than using the AWS IoT MQTT client to publish a message as you did in AWS IoT MQTT Client (p. 29), use something like the following command:

```
    curl --tlsv1.2 --cacert root-CA.crt --cert 4b7828d2e5-certificate.pem.crt --key 4b7828d2e5-private.pem.key -X POST -d "{"serialNumber"": "G030JF053216F1BS", "clickType": "SINGLE", "batteryVoltage": "2000mV" }" https://a1pn10j0v8htvw.iot.us-east-1.amazonaws.com:8443/topics/iotbutton/virtualButton?qos=1

```

```
    --tlsv1.2

    Use TLSv1.2 (SSL). curl must be installed with OpenSSL and you must use version 1.2 of TLS.

    --cacert <filename>

    The filename of the CA certificate to verify the peer.

    --cert <filename>

    The client certificate filename.
```
MQTT Over the WebSocket Protocol

AWS IoT supports MQTT over the WebSocket protocol to enable browser-based and remote applications to send and receive data from AWS IoT-connected devices using AWS credentials. AWS credentials are specified using AWS Signature Version 4. WebSocket support is available on TCP port 443, which allows messages to pass through most firewalls and web proxies.

A WebSocket connection is initiated on a client by sending an HTTP GET request. The URL you use is of the following form:

```
ws://<endpoint>.iot.<region>.amazonaws.com/mqtt
```

- **wss**: Specifies the WebSocket protocol.
- **endpoint**: Your AWS account-specific AWS IoT endpoint. You can use the AWS IoT CLI `describe-endpoint` command to find this endpoint.
- **region**: The AWS region of your AWS account.
- **mqtt**: Specifies you will be sending MQTT messages over the WebSocket protocol.

When the server responds, the client sends an upgrade request to indicate to the server it will communicate using the WebSocket protocol. After the server acknowledges the upgrade request, all communication is performed using the WebSocket protocol. The WebSocket implementation you use acts as a transport protocol. The data you send over the WebSocket protocol are MQTT messages.

**Using the WebSocket Protocol in a Web Application**

The WebSocket implementation provided by most web browsers does not allow the modification of HTTP headers, so you must add the Signature Version 4 information to the query string. For more information, see Adding Signing Information to the Query String.
AWS IoT Developer Guide
MQTT Over the WebSocket Protocol

The following JavaScript deﬁnes some utility functions used in generating a Signature Version 4 request.
/**
* utilities to do sigv4
* @class SigV4Utils
*/
function SigV4Utils() {}
SigV4Utils.getSignatureKey = function (key, date, region, service) {
var kDate = AWS.util.crypto.hmac('AWS4' + key, date, 'buffer');
var kRegion = AWS.util.crypto.hmac(kDate, region, 'buffer');
var kService = AWS.util.crypto.hmac(kRegion, service, 'buffer');
var kCredentials = AWS.util.crypto.hmac(kService, 'aws4_request', 'buffer');
return kCredentials;
};
SigV4Utils.getSignedUrl = function(host, region, credentials) {
var datetime = AWS.util.date.iso8601(new Date()).replace(/[:\-]|\.\d{3}/g, '');
var date = datetime.substr(0, 8);
var
var
var
var
var

method = 'GET';
protocol = 'wss';
uri = '/mqtt';
service = 'iotdevicegateway';
algorithm = 'AWS4-HMAC-SHA256';

var credentialScope = date + '/' + region + '/' + service + '/' + 'aws4_request';
var canonicalQuerystring = 'X-Amz-Algorithm=' + algorithm;
canonicalQuerystring += '&X-Amz-Credential=' +
encodeURIComponent(credentials.accessKeyId + '/' + credentialScope);
canonicalQuerystring += '&X-Amz-Date=' + datetime;
canonicalQuerystring += '&X-Amz-SignedHeaders=host';
var canonicalHeaders = 'host:' + host + '\n';
var payloadHash = AWS.util.crypto.sha256('', 'hex')
var canonicalRequest = method + '\n' + uri + '\n' + canonicalQuerystring + '\n' +
canonicalHeaders + '\nhost\n' + payloadHash;
var stringToSign = algorithm + '\n' + datetime + '\n' + credentialScope + '\n' +
AWS.util.crypto.sha256(canonicalRequest, 'hex');
var signingKey = SigV4Utils.getSignatureKey(credentials.secretAccessKey, date, region,
service);
var signature = AWS.util.crypto.hmac(signingKey, stringToSign, 'hex');
canonicalQuerystring += '&X-Amz-Signature=' + signature;
if (credentials.sessionToken) {
canonicalQuerystring += '&X-Amz-Security-Token=' +
encodeURIComponent(credentials.sessionToken);
}

};

var requestUrl = protocol + '://' + host + uri + '?' + canonicalQuerystring;
return requestUrl;

To create a Signature Version 4 request
1.

Create a canonical request for Signature Version 4.
The following JavaScript code creates a canonical request:
var datetime = AWS.util.date.iso8601(new Date()).replace(/[:\-]|\.\d{3}/g, '');
var date = datetime.substr(0, 8);

168


var method = 'GET';
var protocol = 'wss';
var uri = '/mqtt';
var service = 'iotdevicegateway';
var algorithm = 'AWS4-HMAC-SHA256';

var credentialScope = date + '/' + region + '/' + service + '/' + 'aws4_request';
var canonicalQuerystring = 'X-Amz-Algorithm=' + algorithm;
canonicalQuerystring += '&X-Amz-Credential=' + encodeURIComponent(credentials.accessKeyId + '/' + credentialScope);
canonicalQuerystring += '&X-Amz-Date=' + datetime;
canonicalQuerystring += '&X-Amz-SignedHeaders=host';

2. Create a string to sign, generate a signing key, and sign the string.

Take the canonical URL you created in the previous step and assemble it into a string to sign. You do this by creating a string composed of the hashing algorithm, the date, the credential scope, and the SHA of the canonical request. Next, generate the signing key and sign the string, as shown in the following JavaScript code.

var stringToSign = algorithm + '
' + datetime + '
' + credentialScope + '
' + AWS.util.crypto.sha256(canonicalRequest, 'hex');
var signingKey = SigV4Utils.getSignatureKey(credentials.secretAccessKey, date, region, service);
var signature = AWS.util.crypto.hmac(signingKey, stringToSign, 'hex');

3. Add the signing information to the request.

The following JavaScript code shows how to add the signing information to the query string.

canonicalQuerystring += '&X-Amz-Signature=' + signature;

4. If you have session credentials (from an STS server, AssumeRole, or Amazon Cognito), append the session token to the end of the URL string after signing:

canonicalQuerystring += '&X-Amz-Security-Token=' + encodeURIComponent(credentials.sessionToken);

5. Prepend the protocol, host, and URI to the canonicalQuerystring:

var requestUrl = protocol + '://' + host + uri + '?' + canonicalQuerystring;

6. Open the WebSocket.

The following JavaScript code shows how to create a Paho MQTT client and call CONNECT to AWS IoT. The endpoint argument is your AWS account-specific endpoint. The clientId is a text identifier that is unique among all clients simultaneously connected in your AWS account.

var client = new Paho.MQTT.Client(requestUrl, clientId);
var connectOptions = {
    onSuccess: function(){
        // connect succeeded
    },
    useSSL: true,
    timeout: 3,
    mqttVersion: 4,
    onFailure: function() {
        // connect failed
    }
};
client.connect(connectOptions);

Using the WebSocket Protocol in a Mobile Application

We recommend using one of the AWS IoT Device SDKs to connect your device to AWS IoT when making a WebSocket connection. The following AWS IoT Device SDKs support WebSocket-based MQTT connections to AWS IoT:

- Node.js
- iOS
- Android

For a reference implementation for connecting a web application to AWS IoT using MQTT over the WebSocket protocol, see AWS Labs WebSocket sample.

If you are using a programming or scripting language that is not currently supported, any existing WebSocket library can be used as long as the initial WebSocket upgrade request (HTTP POST) is signed using AWS Signature Version 4. Some MQTT clients, such as Eclipse Paho for JavaScript, support the WebSocket protocol natively.

Topics

The message broker uses topics to route messages from publishing clients to subscribing clients. The forward slash (/) is used to separate topic hierarchy. The following table lists the wildcards that can be used in the topic filter when you subscribe.

<table>
<thead>
<tr>
<th>Wildcard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Must be the last character in the topic to which you are subscribing. Works as a wildcard by matching the current tree and all subtrees. For example, a subscription to Sensor/# will receive messages published to Sensor/, Sensor/temp, Sensor/temp/room1, but not the messages published to Sensor.</td>
</tr>
<tr>
<td>+</td>
<td>Matches exactly one item in the topic hierarchy. For example, a subscription to Sensor/+/room1 will receive messages published to Sensor/temp/room1, Sensor/moisture/room1, and so on.</td>
</tr>
</tbody>
</table>
## Reserved Topics

Any topics beginning with $ are considered reserved and are not supported for publishing and subscribing except for those topics listed below. Any other attempts to publish or subscribe on topics beginning with $ will result in a terminated connection.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Allowed Operations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>$aws/events/presence/connected/clientId</code></td>
<td>Subscribe</td>
<td>AWS IoT publishes to this topic when an MQTT client with the specified client ID connects to AWS IoT. For more information, see Connect/Disconnect Events (p. 174).</td>
</tr>
<tr>
<td><code>$aws/events/presence/disconnected/clientId</code></td>
<td>Subscribe</td>
<td>AWS IoT publishes to this topic when an MQTT client with the specified client ID disconnects to AWS IoT. For more information, see Connect/Disconnect Events (p. 174).</td>
</tr>
<tr>
<td><code>$aws/events/subscriptions/subscribed/clientId</code></td>
<td>Subscribe</td>
<td>AWS IoT publishes to this topic when an MQTT client with the specified client ID subscribes to an MQTT topic. For more information, see Subscribe/Unsubscribe Events (p. 174).</td>
</tr>
<tr>
<td><code>$aws/events/subscriptions/unsubscribed/clientId</code></td>
<td>Subscribe</td>
<td>AWS IoT publishes to this topic when an MQTT client with the specified client ID unsubscribes to an MQTT topic. For more information, see Subscribe/Unsubscribe Events (p. 174).</td>
</tr>
<tr>
<td><code>$aws/things/thingName/shadow/delete</code></td>
<td>Publish/Subscribe</td>
<td>A device or an application publishes to this topic to delete a shadow. For more information see <a href="http://docs.aws.amazon.com/iot/latest/developerguide/device-shadow-mqtt.html#delete-pub-sub-topic">http://docs.aws.amazon.com/iot/latest/developerguide/device-shadow-mqtt.html#delete-pub-sub-topic</a>.</td>
</tr>
<tr>
<td><code>$aws/things/thingName/shadow/delete/accepted</code></td>
<td>Subscribe</td>
<td>The Device Shadow service sends messages to this topic when a shadow is deleted. For more information, see <a href="http://docs.aws.amazon.com/iot/latest/developerguide/device-shadow-">http://docs.aws.amazon.com/iot/latest/developerguide/device-shadow-</a>.</td>
</tr>
<tr>
<td>Topic</td>
<td>Allowed Operations</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>$aws/things/thingName/shadow/delete/rejected</td>
<td>Subscribe</td>
<td>The Device Shadow service sends messages to this topic when a request to delete a shadow is rejected. For more information, see <a href="http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html#delete-rejected-pub-sub-topic.">http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html#delete-rejected-pub-sub-topic.</a></td>
</tr>
<tr>
<td>$aws/things/thingName/shadow/get</td>
<td>Publish/Subscribe</td>
<td>An application or a thing publishes an empty message to this topic to get a shadow. For more information, see <a href="http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html">http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html</a>.</td>
</tr>
<tr>
<td>$aws/things/thingName/shadow/get/accepted</td>
<td>Subscribe</td>
<td>The Device Shadow service sends messages to this topic when a request for a shadow is made successfully. For more information, see <a href="http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html#get-accepted-pub-sub-topic.">http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html#get-accepted-pub-sub-topic.</a></td>
</tr>
<tr>
<td>$aws/things/thingName/shadow/get/rejected</td>
<td>Subscribe</td>
<td>The Device Shadow service sends messages to this topic when a request for a shadow is rejected. For more information, see <a href="http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html#get-rejected-pub-sub-topic.">http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html#get-rejected-pub-sub-topic.</a></td>
</tr>
<tr>
<td>$aws/things/thingName/shadow/update</td>
<td>Publish/Subscribe</td>
<td>A thing or application publishes to this topic to update a shadow. For more information, see <a href="http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html#update-pub-sub-topic.">http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html#update-pub-sub-topic.</a></td>
</tr>
<tr>
<td>Topic</td>
<td>Allowed Operations</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>$aws/things/thingName/shadow/update/accepted</td>
<td>Subscribe</td>
<td>The Device Shadow service sends messages to this topic when an update is successfully made to a shadow. For more information, see <a href="http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html#update-accepted-pub-sub-topic">http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html#update-accepted-pub-sub-topic</a>.</td>
</tr>
<tr>
<td>$aws/things/thingName/shadow/update/rejected</td>
<td>Subscribe</td>
<td>The Device Shadow service sends messages to this topic when an update to a shadow is rejected. For more information, see <a href="http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html#update-rejected-pub-sub-topic">http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html#update-rejected-pub-sub-topic</a>.</td>
</tr>
<tr>
<td>$aws/things/thingName/shadow/update/delta</td>
<td>Subscribe</td>
<td>The Device Shadow service sends messages to this topic when a difference is detected between the reported and desired sections of a shadow. For more information, see <a href="http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html#update-delta-pub-sub-topic">http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html#update-delta-pub-sub-topic</a>.</td>
</tr>
<tr>
<td>$aws/things/thingName/shadow/update/documents</td>
<td>Subscribe</td>
<td>AWS IoT publishes a state document to this topic whenever an update to the shadow is successfully performed. For more information, see <a href="http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html#update-documents-pub-sub-topic">http://docs.aws.amazon.com/iot/latest/developerguide//device-shadow-mqtt.html#update-documents-pub-sub-topic</a>.</td>
</tr>
</tbody>
</table>

**Lifecycle Events**

AWS IoT publishes lifecycle events on the MQTT topics discussed in the following sections. These messages allow you to be notified of lifecycle events from the message broker.

**Note**
Life cycle messages might be sent out of order. You might receive duplicate messages.
Connect/Disconnect Events

AWS IoT publishes a message to the following MQTT topics when a client connects or disconnects:

```markdown
/aws/events/presence/connected/clientId
```

or

```markdown
/aws/events/presence/disconnected/clientId
```

Where `clientId` is the MQTT client ID that connects to or disconnects from the AWS IoT message broker.

The message published to this topic has the following structure:

```json
{
    "clientId": "a1b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6",
    "timestamp": 1460065214626,
    "eventType": "connected",
    "sessionIdentifier": "00000000-0000-0000-0000-000000000000",
    "principalIdentifier": "000000000000/ABCDEFGHIJKLMNOPQRSTU:some-user/ABCDEFGHIJKLMNOPQRSTU:some-user"
}
```

The following is a list of JSON elements that are contained in the connection/disconnection messages published to the `/aws/events/presence/connected/clientId` topic.

- **clientId**
  The client ID of the connecting or disconnecting client.
  
  **Note**
  Client IDs that contain # or + do not receive lifecycle events.

- **clientInitiatedDisconnect**
  Only found in disconnection messages. True if the client initiated the disconnect, otherwise False.

- **eventType**
  The type of event. Valid values are `connected` or `disconnected`.

- **principalIdentifier**
  The credential used to authenticate. For TLS mutual authentication certificates, this is the certificate ID. For other connections, this is IAM credentials.

- **sessionIdentifier**
  A globally unique identifier in AWS IoT that exists for the life of the session.

- **timestamp**
  An approximation of when the event occurred, expressed in milliseconds since the Unix epoch. The accuracy of the timestamp is +/- 2 minutes.

Subscribe/Unsubscribe Events

AWS IoT publishes a message to the following MQTT topic when a client subscribes or unsubscribes to an MQTT topic:
Where `clientId` is the MQTT client ID that connects to the AWS IoT message broker.

The message published to this topic has the following structure:

```
{
  "clientId": "186b5",
  "timestamp": 1460065214626,
  "eventType": "subscribed" | "unsubscribed",
  "sessionIdentifier": "00000000-0000-0000-0000-000000000000",
  "principalIdentifier": "000000000000/ABCDEFGHIJKLMNOPQRSTU:some-user/ABCDEFHIGJKLMNOPQRSTUVWXYZ:some-user",
  "topics" : 
["foo/bar","device/data","dog/cat"]
}
```

The following is a list of JSON elements that are contained in the subscribed and unsubscribed messages published to the `$aws/events/subscriptions/subscribed/clientId` and `$aws/events/subscriptions/unsubscribed/clientId` topics.

**ClientId**
- The client ID of the subscribing or unsubscribing client.

**Note**
- Client IDs that contain # or + do not receive lifecycle events.

**EventType**
- The type of event. Valid values are `subscribed` or `unsubscribed`.

**PrincipalIdentifier**
- The credential used to authenticate. For TLS mutual authentication certificates, this is the certificate ID. For other connections, this is IAM credentials.

**SessionIdentifier**
- A globally unique identifier in AWS IoT that exists for the life of the session.

**Timestamp**
- An approximation of when the event occurred, expressed in milliseconds since the Unix epoch. The accuracy of the timestamp is +/- 2 minutes.

**Topics**
- An array of the MQTT topics to which the client has subscribed.

**Note**
- Lifecycle messages might be sent out of order. You might receive duplicate messages.
Rules for AWS IoT

Rules give your devices the ability to interact with AWS services. Rules are analyzed and actions are performed based on the MQTT topic stream. You can use rules to support tasks like these:

- Augment or filter data received from a device.
- Write data received from a device to an Amazon DynamoDB database.
- Save a file to Amazon S3.
- Send a push notification to all users using Amazon SNS.
- Publish data to an Amazon SQS queue.
- Invoke a Lambda function to extract data.
- Process messages from a large number of devices using Amazon Kinesis.
- Send data to the Amazon Elasticsearch Service.
- Capture a CloudWatch metric.
- Change a CloudWatch alarm.
- Send the data from an MQTT message to Amazon Machine Learning to make predictions based on an Amazon ML model.
- Send a message to a Salesforce IoT Input Stream.
- Send message data to an AWS IoT Analytics channel.
- Start execution of a Step Functions state machine.

Before AWS IoT can perform these actions, you must grant it permission to access your AWS resources on your behalf. When the actions are performed, you incur the standard charges for the AWS services you use.

Contents
- Granting AWS IoT the Required Access (p. 176)
- Pass Role Permissions (p. 178)
- Creating an AWS IoT Rule (p. 178)
- Viewing Your Rules (p. 182)
- SQL Versions (p. 182)
- Troubleshooting a Rule (p. 184)
- Rule Error Handling (p. 184)
- Deleting a Rule (p. 186)
- AWS IoT Rule Actions (p. 186)
- AWS IoT SQL Reference (p. 200)

Granting AWS IoT the Required Access

You use IAM roles to control the AWS resources to which each rule has access. Before you create a rule, you must create an IAM role with a policy that allows access to the required AWS resources. AWS IoT assumes this role when executing a rule.

To create an IAM role (AWS CLI)

1. Save the following trust policy document, which grants AWS IoT permission to assume the role, to a file called iot-role-trust.json:
AWS IoT Developer Guide  
Granting AWS IoT the Required Access

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "Service": "iot.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
    }]
}
```

Use the `create-role` command to create an IAM role specifying the `iot-role-trust.json` file:

```bash
aws iam create-role --role-name my-iot-role --assume-role-policy-document file://iot-role-trust.json
```

The output of this command looks like the following:

```json
{
    "Role": {
        "AssumeRolePolicyDocument": "url-encoded-json",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "CreateDate": "2015-09-30T18:43:32.821Z",
        "RoleName": "my-iot-role",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/my-iot-role"
    }
}
```

2. Save the following JSON into a file named `iot-policy.json`.

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": "dynamodb:*",
        "Resource": "*"
    }]
}
```

This JSON is an example policy document that grants AWS IoT administrator access to DynamoDB.

Use the `create-policy` command to grant AWS IoT access to your AWS resources upon assuming the role, passing in the `iot-policy.json` file:

```bash
aws iam create-policy --policy-name my-iot-policy --policy-document file://my-iot-policy.json
```

For more information about how to grant access to AWS services in policies for AWS IoT, see Creating an AWS IoT Rule (p. 178).

The output of the `create-policy` command contains the ARN of the policy. You need to attach the policy to a role.

```json
{
    "Policy": {
        "PolicyName": "my-iot-policy",
        "CreateDate": "2015-09-30T19:31:18.620Z",
    }
}
```
3. Use the `attach-role-policy` command to attach your policy to your role:

```bash
aws iam attach-role-policy --role-name my-iot-role --policy-arn "arn:aws:iam::123456789012:policy/my-iot-policy"
```

### Pass Role Permissions

Part of a rule definition is an IAM role that grants permission to access resources specified in the rule's action. The rules engine assumes that role when the rule's action is triggered. The role must be defined in the same AWS account as the rule.

When creating or replacing a rule you are, in effect, passing a role to the rules engine. The user performing this operation requires the `iam:PassRole` permission. To ensure you have this permission, create a policy that grants the `iam:PassRole` permission and attach it to your IAM user. The following policy shows how to allow `iam:PassRole` permission for a role.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::123456789012:role/myRole"
            ]
        }
    ]
}
```

In this policy example, the `iam:PassRole` permission is granted for the role `myRole`. The role is specified using the role's ARN. You must attach this policy to your IAM user or role to which your user belongs. For more information, see [Working with Managed Policies](#).

**Note**

Lambda functions use resource-based policy, where the policy is attached directly to the Lambda function itself. When creating a rule that invokes a Lambda function, you do not pass a role, so the user creating the rule does not need the `iam:PassRole` permission. For more information about Lambda function authorization, see [Granting Permissions Using a Resource Policy](#).

### Creating an AWS IoT Rule

You configure rules to route data from your connected things. Rules consist of the following:
Rule name

The name of the rule.

Optional description

A textual description of the rule.

SQL statement

A simplified SQL syntax to filter messages received on an MQTT topic and push the data elsewhere. For more information, see AWS IoT SQL Reference (p. 200).

SQL version

The version of the SQL rules engine to use when evaluating the rule. Although this property is optional, we strongly recommend that you specify the SQL version. If this property is not set, the default, 2015-10-08, is used.

One or more actions

The actions AWS IoT performs when executing the rule. For example, you can insert data into a DynamoDB table, write data to an Amazon S3 bucket, publish to an Amazon SNS topic, or invoke a Lambda function.

An error action

The action AWS IoT performs when it is unable to perform a rule's action.

When you create a rule, be aware of how much data you are publishing on topics. If you create rules that include a wildcard topic pattern, they might match a large percentage of your messages, and you might need to increase the capacity of the AWS resources used by the target actions. Also, if you create a republish rule that includes a wildcard topic pattern, you can end up with a circular rule that causes an infinite loop.

**Note**

Creating and updating rules are administrator-level actions. Any user who has permission to create or update rules is able to access data processed by the rules.

**To create a rule (AWS CLI)**

Use the `create-topic-rule` command to create a rule:

```
aws iot create-topic-rule --rule-name my-rule --topic-rule-payload file://my-rule.json
```

The following is an example payload file with a rule that inserts all messages sent to the `iot/test` topic into the specified DynamoDB table. The SQL statement filters the messages and the role ARN grants AWS IoT permission to write to the DynamoDB table.

```json
{
  "sql": "SELECT * FROM 'iot/test'",
  "ruleDisabled": false,
  "awsIoTSqlVersion": "2016-03-23",
  "actions": [{
    "dynamoDB": {
      "tableName": "my-dynamodb-table",
      "roleArn": "arn:aws:iam::123456789012:role/my-iot-role",
      "hashKeyField": "topic",
      "hashKeyValue": 

"topic(2)}",
      "rangeKeyField": "timestamp",
      "rangeKeyValue": "${timestamp()}
    }
  }
}
```
The following is an example payload file with a rule that inserts all messages sent to the `iot/test` topic into the specified S3 bucket. The SQL statement filters the messages, and the role ARN grants AWS IoT permission to write to the Amazon S3 bucket.

```json
{
    "awsIotSqlVersion": "2016-03-23",
    "sql": "SELECT * FROM 'iot/test'",
    "ruleDisabled": false,
    "actions": [
        {
            "s3": {
                "roleArn": "arn:aws:iam::123456789012:role/aws_iot_s3",
                "bucketName": "my-bucket",
                "key": "myS3Key"
            }
        }
    ]
}
```

The following is an example payload file with a rule that pushes data to Amazon ES:

```json
{
    "sql": "SELECT *, timestamp() as timestamp FROM 'iot/test'",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [
        {
            "elasticsearch": {
                "roleArn": "arn:aws:iam::123456789012:role/aws_iot_es",
                "endpoint": "https://my-endpoint",
                "index": "my-index",
                "type": "my-type",
                "id": "${newuuid()}"
            }
        }
    ]
}
```

The following is an example payload file with a rule that invokes a Lambda function:

```json
{
    "sql": "expression",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [{
        "lambda": {
            "functionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-lambda-function"
        }
    }]
}
```

The following is an example payload file with a rule that publishes to an Amazon SNS topic:

```json
{
    "sql": "expression",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [{
        "sns": {
            "topicArn": "arn:aws:sns:us-west-2:123456789012:my-topic"
        }
    }]
}
```
The following is an example payload file with a rule that republishes on a different MQTT topic:

```json
{
    "sql": "expression",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [{
        "republish": {
            "roleArn": "arn:aws:iam::123456789012:role/my-iot-role",
            "topic": "my-mqtt-topic"
        }
    }]
}
```

The following is an example payload file with a rule that pushes data to an Amazon Kinesis Data Firehose stream:

```json
{
    "sql": "SELECT * FROM 'my-topic'",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [{
        "firehose": {
            "roleArn": "arn:aws:iam::123456789012:role/my-iot-role",
            "deliveryStreamName": "my-stream-name"
        }
    }]
}
```

The following is an example payload file with a rule that uses the Amazon Machine Learning machinelearning_predict function to republish to a topic if the data in the MQTT payload is classified as a 1.

```json
{
    "sql": "SELECT * FROM 'iot/test' where machinelearning_predict('my-model', 'arn:aws:iam::123456789012:role/my-iot-aml-role', *).predictedLabel=1",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [{
        "republish": {
            "roleArn": "arn:aws:iam::123456789012:role/my-iot-role",
            "topic": "my-mqtt-topic"
        }
    }]
}
```

The following is an example payload file with a rule that publishes messages to a Salesforce IoT Cloud input stream:

```json
{
    "sql": "expression",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [{
        "firehose": {
            "roleArn": "arn:aws:iam::123456789012:role/my-iot-role",
            "deliveryStreamName": "my-stream-name"
        }
    }]
}
```
The following is an example payload file with a rule that starts an execution of a Step Functions state machine.

```json
{
    "sql": "expression",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [{
        "stepFunctions": {
            "stateMachineName": "myCoolStateMachine",
            "executionNamePrefix": "coolRunning",
            "roleArn": "arn:aws:iam::123456789012:role/my-iot-role"
        }
    }]
}
```

**SQL Versions**

The AWS IoT rules engine uses an SQL-like syntax to select data from MQTT messages. The SQL statements are interpreted based on an SQL version specified with the `awsIotSqlVersion` property in a JSON document that describes the rule. For more information about the structure of JSON rule documents, see Creating a Rule (p. 178). The `awsIotSqlVersion` property allows you to specify which version of the AWS IoT SQL rules engine you want to use. When a new version is deployed, you can continue to use an older version or change your rule to use the new version. Your current rules continue to use the version with which they were created.

The following JSON example shows how to specify the SQL version using the `awsIotSqlVersion` property:

```json
{
    "sql": "expression",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [{
        "republish": {
```
Current supported versions are:

- **2015-10-08**, the original SQL version built on 2015-10-08.
- **2016-03-23**, the SQL version built on 2016-03-23.
- **beta**, the most recent beta SQL version. The use of this version might introduce breaking changes to your rules.

### What's New in the 2016-03-23 SQL Rules Engine Version

- Fixes for selecting nested JSON objects.
- Fixes for array queries.
- Inter-object query support.
- Support to output an array as a top-level object.
- Adds the encode (\textit{value}, \textit{encodingScheme}) function, which can be applied on both JSON and non-JSON format data.

### Inter-Object Queries

This feature allows you to query for an attribute in a JSON object. For example, given the following MQTT message:

```json
{
    "e": [
        { "n": "temperature", "u": "Cel", "t": 1234, "v":22.5 },
        { "n": "light", "u": "lm", "t": 1235, "v":135 },
        { "n": "acidity", "u": "pH", "t": 1235, "v":7 }
    ]
}
```

And the following rule:

```sql
SELECT (SELECT v FROM e WHERE n = 'temperature') as temperature FROM 'my/topic'
```

The rule generates the following output:

```json
{"temperature": [{"v":22.5}]}
```

Using the same MQTT message, given a slightly more complicated rule such as:

```sql
SELECT get((SELECT v FROM e WHERE n = 'temperature'),1).v as temperature FROM 'topic'
```

The rule generates the following output:

```json
{"temperature":22.5}
```
Output an Array as a Top-Level Object

This feature allows a rule to return an array as a top-level object. For example, given the following MQTT message:

```json
{
   "a": {"b":"c"},
   "arr":[1,2,3,4]
}
```

And the following rule:

```sql
SELECT VALUE arr FROM 'topic'
```

The rule generates the following output:

```
[1,2,3,4]
```

Encode Function

Encodes the payload, which potentially might be non-JSON data, into its string representation based on the specified encoding scheme.

Troubleshooting a Rule

If you are having an issue with your rules, you should enable CloudWatch Logs. By analyzing your logs, you can determine whether the issue is authorization or whether, for example, a WHERE clause condition did not match. For more information about using Amazon CloudWatch Logs, see Setting Up CloudWatch Logs.

Rule Error Handling

When AWS IoT receives a message from a device, the Rules Engine checks to see if the message matches a rule. If so, the rule's SQL statement is evaluated and the rule's actions are invoked, passing the SQL statement's result.

If a problem occurs when invoking an action, the Rules Engine will invoke an error action, if one is specified for the rule. This may happen when, for example:

- A rule doesn't have permission to access an Amazon S3 bucket.
- A user error causes DynamoDB provisioned throughput to be exceeded.

Error Action Message Format

A single message is generated per rule and message. For example, if two rule actions in the same rule fail, the error action will receive one message containing both errors.

The error action message will look like this:

```json
{
   "ruleName": "TestAction",
```


ruleName
The name of the rule that triggered the error action.

topic
The topic on which the original message was received.

cloudwatchTraceId
A unique identity referring to the error logs in CloudWatch.

clientId
The client ID of the message publisher.

base64OriginalPayload
The original message payload base64 encoded.

failures

failedAction
The name of the action that failed to complete, for example "S3Action".

failedResource
The name of the resource, for example the name of an S3 bucket.

eerrorMessage
The description and explanation of the error.

Error Action Example

Here is an example of a rule with an added error action. The following rule has an action that writes message data to a DynamoDB table and an error action that writes data to an Amazon S3 bucket:

```json
{  
  "sql" : "SELECT * FROM ... 
  "actions" : [{  
    "dynamoDB" : {  
      "table" : "PoorlyConfiguredTable",  
      "hashKeyField" : "AConstantString",  
      "hashKeyValue" : "AHashKey"}  
  }  
}  
```

Deleting a Rule

When you are finished with a rule, you can delete it.

To delete a rule (AWS CLI)

Use the `delete-topic-rule` command to delete a rule:

```
aws iot delete-topic-rule --rule-name my-rule
```

AWS IoT Rule Actions

AWS IoT rule actions are used to specify what to do when a rule is triggered. You can define actions to write data to a DynamoDB database or a Kinesis stream or to invoke a Lambda function, and more. The following actions are supported:

- `cloudwatchAlarm` to change a CloudWatch alarm.
- `cloudwatchMetric` to capture a CloudWatch metric.
- `dynamoDB` to write data to a DynamoDB database.
- `dynamoDBv2` to write data to a DynamoDB database.
- `elasticsearch` to write data to an Amazon Elasticsearch Service domain.
- `firehose` to write data to an Amazon Kinesis Data Firehose stream.
- `iotAnalytics` to send data to an AWS IoT Analytics channel.
- `kinesis` to write data to a Kinesis stream.
- `lambda` to invoke a Lambda function.
- `republish` to republish the message on another MQTT topic.
- `s3` to write data to an Amazon S3 bucket.
- `salesforce` to write data to a Salesforce IoT input stream.
- `sns` to write data as a push notification.
- `sqs` to write data to an SQS queue.
- `stepFunctions` to start execution of a Step Functions state machine.

**Note**
The AWS IoT rules engine does not currently retry delivery for messages that fail to be published to another service.

You can use any function or substitution in an error action's SQL statement, except for external functions (for example, `get_thing_shadow`, `aws_lambda`, and `machinelearning_predict`).

For more information about rules and how to specify an error action, see Creating an AWS IoT Rule.

For more information on using CloudWatch to monitor the success or failure of rules, see AWS IoT Metrics and Dimensions (p. 540).
The following discusses each action in detail.

**CloudWatch Alarm Action**

The CloudWatch alarm action allows you to change CloudWatch alarm state. You can specify the state change reason and value in this call.

When creating an AWS IoT rule with a CloudWatch alarm action, you must specify the following information:

- **roleArn**
  The IAM role that allows access to the CloudWatch alarm.

- **alarmName**
  The CloudWatch alarm name.

- **stateReason**
  Reason for the alarm change.

- **stateValue**
  The value of the alarm state. Acceptable values are OK, ALARM, INSUFFICIENT_DATA.

**Note**
Ensure the role associated with the rule has a policy that grants the cloudwatch:SetAlarmState permission.

The following JSON example shows how to define a CloudWatch alarm action in an AWS IoT rule:

```json
{
  "rule": {
    "sql": "SELECT * FROM 'some/topic'",
    "ruleDisabled": false,
    "actions": [{
      "cloudwatchAlarm": {
        "roleArn": "arn:aws:iam::123456789012:role/aws_iot_cw",
        "alarmName": "IotAlarm",
        "stateReason": "Temperature stabilized.",
        "stateValue": "OK"
      }
    }]
  }
}
```

For more information, see CloudWatch Alarms.

**CloudWatch Metric Action**

The CloudWatch metric action allows you to capture a CloudWatch metric. You can specify the metric namespace, name, value, unit, and timestamp.
When creating an AWS IoT rule with a CloudWatch metric action, you must specify the following information:

- **roleArn**
  The IAM role that allows access to the CloudWatch metric.

- **metricNamespace**
  CloudWatch metric namespace name.

- **metricName**
  The CloudWatch metric name.

- **metricValue**
  The CloudWatch metric value.

- **metricUnit**
  The metric unit supported by CloudWatch.

- **metricTimestamp**
  An optional Unix timestamp.

**Note**
Ensure the role associated with the rule has a policy granting the `cloudwatch:PutMetricData` permission.

The following JSON example shows how to define a CloudWatch metric action in an AWS IoT rule:

```json
{
    "rule": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "actions": [{
            "cloudwatchMetric": {
                "roleArn": "arn:aws:iam::123456789012:role/aws_iot_cw",
                "metricNamespace": "IotNamespace",
                "metricName": "IotMetric",
                "metricValue": "1",
                "metricUnit": "Count",
                "metricTimestamp": "1456821314"
            }
        }
    }
}
```

For more information, see [CloudWatch Metrics](#).

## DynamoDB Action

The **DynamoDB** action allows you to write all or part of an MQTT message to a DynamoDB table.

When creating a DynamoDB rule, you must specify the following information:
hashKeyType

The data type of the hash key (also called the partition key). Valid values are: "STRING" or "NUMBER".

hashKeyField

The name of the hash key (also called the partition key).

hashKeyValue

The value of the hash key.

rangeKeyType

Optional. The data type of the range key (also called the sort key). Valid values are: "STRING" or "NUMBER".

rangeKeyField

Optional. The name of the range key (also called the sort key).

rangeKeyValue

Optional. The value of the range key.

operation

Optional. The type of operation to be performed. This follows the substitution template, so it can be `${operation}`, but the substitution must result in one of the following: INSERT, UPDATE, or DELETE.

payloadField

Optional. The name of the field where the payload is written. If this value is omitted, the payload is written to the `payload` field.

table

The name of the DynamoDB table.

roleARN

The IAM role that allows access to the DynamoDB table. At a minimum, the role must allow the `dynamodb:PutItem` IAM action.

The data written to the DynamoDB table is the result from the SQL statement of the rule. The `hashKeyValue` and `rangeKeyValue` fields are usually composed of expressions (for example, `${topic()}` or `${timestamp()}`).

**Note**

Non-JSON data is written to DynamoDB as binary data. The DynamoDB console displays the data as Base64-encoded text.

Ensure the role associated with the rule has a policy granting the `dynamodb:PutItem` permission.

The following JSON example shows how to define a `dynamoDB` action in an AWS IoT rule:

```json
{
  "rule": {
    "ruleDisabled": false,
    "sql": "SELECT * AS message FROM 'some/topic'",
    "description": "A test Dynamo DB rule",
    "actions": [
```
DynamoDBv2 Action

DynamoDBv2 Action

The `dynamoDBv2` action allows you to write all or part of an MQTT message to a DynamoDB table. Each attribute in the payload is written to a separate column in the DynamoDB database.

When creating a DynamoDB rule, you must specify the following information:

- **roleARN**
  
The IAM role that allows access to the DynamoDB table. At a minimum, the role must allow the `dynamoDB:PutItem` IAM action.

- **tableName**
  
The name of the DynamoDB table.

**Note**

The MQTT message payload must contain a root-level key that matches the table's primary partition key and a root-level key that matches the table's primary sort key, if one is defined.

The data written to the DynamoDB table is the result from the SQL statement of the rule.

**Note**

Ensure the role associated with the rule has a policy granting the `dynamodb:PutItem` permission.

The following JSON example shows how to define a `dynamoDB` action in an AWS IoT rule:

```json
{
  "rule": {
    "ruleDisabled": false,
    "sql": "SELECT * AS message FROM 'some/topic'",
    "description": "A test DynamoDBv2 rule",
    "actions": [
      { "dynamoDBv2": {
        "roleArn": "arn:aws:iam::123456789012:role/aws_iot_dynamoDBv2",
        "putItem": {
          "tableName": "my_ddb_table"
        }
      }]
  }
}
```
Amazon ES Action

The `elasticsearch` action allows you to write data from MQTT messages to an Amazon Elasticsearch Service domain. Data in Amazon ES can then be queried and visualized by using tools like Kibana.

When you create an AWS IoT rule with an `elasticsearch` action, you must specify the following information:

- **endpoint**
  The endpoint of your Amazon ES domain.

- **index**
  The Amazon ES index where you want to store your data.

- **type**
  The type of document you are storing.

- **id**
  The unique identifier for each document.

**Note**
Ensure the role associated with the rule has a policy granting the `es:ESHttpPut` permission.

The following JSON example shows how to define an `elasticsearch` action in an AWS IoT rule:

```json
{
    "rule":{
        "sql":"SELECT *, timestamp() as timestamp FROM 'iot/test'",
        "ruleDisabled":false,
        "actions":[
            {
                "elasticsearch":{
                    "roleArn":"arn:aws:iam::123456789012:role/aws_iot_es",
                    "endpoint":"https://my-endpoint",
                    "index":"my-index",
                    "type":"my-type",
                    "id":"${newuuid()}"
                }
            }
        ]
    }
}
```

For more information, see the Amazon ES Developer Guide.
Firehose Action

Firehose Action

A firehose action sends data from an MQTT message that triggered the rule to a Kinesis Data Firehose stream.

more info (6)

When creating a rule with a firehose action, you must specify the following information:

deliveryStreamName

The Kinesis Data Firehose stream to which to write the message data.

roleArn

The IAM role that allows access to Kinesis Data Firehose.

separator

A character separator that is used to separate records written to the Firehose stream. Valid values are: ‘\n’ (newline), ‘\t’ (tab), ‘\r\n’ (Windows newline), ‘,’ (comma).

Note

Make sure the role associated with the rule has a policy that grants the firehose:PutRecord permission.

The following JSON example shows how to create an AWS IoT rule with a firehose action:

```
{
   "rule": {
       "sql": "SELECT * FROM 'some/topic'",
       "ruleDisabled": false,
       "actions": [{
           "firehose": {
               "roleArn": "arn:aws:iam::123456789012:role/aws_iot_firehose",
               "deliveryStreamName": "my_firehose_stream"
           }
       }]
   }
}
```

For more information, see the Kinesis Data Firehose Developer Guide.

IoT Analytics Action

IoT Analytics Action

An iotAnalytics action sends data from the MQTT message that triggered the rule to an AWS IoT Analytics channel.

more info (7)

When creating a rule with an iotAnalytics action, you must specify the following information:

channelName

The name of the AWS IoT Analytics channel to which to write the data.
roleArn

The IAM role that allows access to the AWS IoT Analytics channel.

The policy attached to the role you specify should look like this:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iotanalytics:BatchPutMessage",
            "Resource": [
                "arn:aws:iotanalytics:us-west-2:<your-account-number>:channel/mychannel"
            ]
        }
    ]
}
```

and have a trust relationship that looks like this:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "iot.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
        }
    ]
}
```

The following JSON example shows how to create an AWS IoT rule with an `iotAnalytics` action:

```json
{
    "rule": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [{
            "iotAnalytics": {
                "channelName": "mychannel",
                "roleArn": "arn:aws:iam::123456789012:role/analyticsRole",
            }
        }]
    }
}
```

For more information, see the AWS IoT Analytics User Guide.

### Kinesis Action

The `kinesis` action allows you to write data from MQTT messages into a Kinesis stream.
When creating an AWS IoT rule with a `kinesis` action, you must specify the following information:

- **stream**
  The Kinesis stream to which to write data.

- **partitionKey**
  The partition key used to determine to which shard the data is written. The partition key is usually composed of an expression (for example,`${topic()}` or `${timestamp()}`).

**Note**
Ensure that the policy associated with the rule has the `kinesis:PutRecord` permission.

The following JSON example shows how to define a `kinesis` action in an AWS IoT rule:

```json
{
  "rule": {
    "sql": "SELECT * FROM 'some/topic'",
    "ruleDisabled": false,
    "actions": [{
      "kinesis": {
        "roleArn": "arn:aws:iam::123456789012:role/aws_iot_kinesis",
        "streamName": "my_kinesis_stream",
        "partitionKey": `${topic()}`
      }
    }]
  }
}
```

For more information, see the Kinesis Developer Guide.

Lambda Action

A lambda action calls a Lambda function, passing in the MQTT message that triggered the rule.

In order for AWS IoT to call a Lambda function, you must configure a policy granting the `lambda:InvokeFunction` permission to AWS IoT. Lambda functions use resource-based policies, so you must attach the policy to the Lambda function itself. Use the following CLI command to attach a policy granting `lambda:InvokeFunction` permission:

```bash
aws lambda add-permission --function-name "function_name" --region "region" --principal iot.amazonaws.com --source-arn arn:aws:iot:us-east-2:account_id:rule/rule_name --source-account "account_id" --statement-id "unique_id" --action "lambda:InvokeFunction"
```

The following are the arguments for the `add-permission` command:

- **--function-name**
  Name of the Lambda function whose resource policy you are updating by adding a new permission.

- **--region**
  The AWS region of your account.
--principal

The principal who is getting the permission. This should be `iot.amazonaws.com` to allow AWS IoT permission to call a Lambda function.

--source-arn

The ARN of the rule. You can use the `get-topic-rule` CLI command to get the ARN of a rule.

--source-account

The AWS account where the rule is defined.

--statement-id

A unique statement identifier.

--action

The Lambda action you want to allow in this statement. In this case, we want to allow AWS IoT to invoke a Lambda function, so we specify `lambda:InvokeFunction`.

**Note**

If you add a permission for an AWS IoT principal without providing the source ARN, any AWS account that creates a rule with your Lambda action can trigger rules to invoke your Lambda function from AWS IoT.

For more information, see [Lambda Permission Model](#).

When creating a rule with a `lambda` action, you must specify the Lambda function to invoke when the rule is triggered.

The following JSON example shows a rule that calls a Lambda function:

```json
{
  "rule": {
    "sql": "SELECT * FROM 'some/topic'",
    "ruleDisabled": false,
    "actions": [{
      "lambda": {
        "functionArn": "arn:aws:lambda:us-east-2:123456789012:function:myLambdaFunction"
      }
    }
  }
}
```

For more information, see the [AWS Lambda Developer Guide](#).

### Republish Action

Republish Action

The `republish` action allows you to republish the message that triggered the role to another MQTT topic.

When creating a rule with a `republish` action, you must specify the following information:

**topic**

The MQTT topic to which to republish the message.
roleArn

The IAM role that allows publishing to the MQTT topic.

**Note**

Make sure the role associated with the rule has a policy granting the `iot:Publish` permission.

```json
{
"rule": {
  "sql": "SELECT * FROM 'some/topic'",
  "ruleDisabled": false,
  "actions": [{
    "republish": {
      "topic": "another/topic",
      "roleArn": "arn:aws:iam::123456789012:role/aws_iot_republish"
    }
  }
}
}
```

S3 Action

S3 Action

An `s3` action writes the data from the MQTT message that triggered the rule to an Amazon S3 bucket.

more info (11)

When creating an AWS IoT rule with an `s3` action, you must specify the following information (except for `cannedacl`, which is optional):

**bucket**

The Amazon S3 bucket to which to write data.

**cannedacl**

The Amazon S3 canned ACL that controls access to the object identified by the object key. For more information, see S3 Canned ACLs (which lists the allowed values). Note that `cannedacl` is optional.

**key**

The path to the file where the data is written. For example, if the value of this argument is `"${topic()}/${timestamp()}"`, the topic the message was sent to is "this/is/my/topic," and the current timestamp is 1460685389, the data is written to a file called "1460685389" in the "this/is/my/topic" folder on Amazon S3.

**Note**

Using a static key results in a single file in Amazon S3 being overwritten for each invocation of the rule. More common use cases are to use the message timestamp or another unique message identifier, so that a new file is saved in Amazon S3 for each message received.

**roleArn**

The IAM role that allows access to the Amazon S3 bucket.
Note
Make sure the role associated with the rule has a policy granting the `s3:PutObject` permission.

The following JSON example shows how to define an `s3` action in an AWS IoT rule:

```json
{
    "rule": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "actions": [{
            "s3": {
                "roleArn": "arn:aws:iam::123456789012:role/aws_iot_s3",
                "bucketName": "my-bucket",
                "key": "#{topic()}#{timestamp()}",
                "cannedacl": "public-read"
            }
        }]
    }
}
```

For more information, see the Amazon S3 Developer Guide.

Salesforce Action

A salesforce action sends data from the MQTT message that triggered the rule to a Salesforce IoT Input Stream. When creating a rule with a salesforce action, you must specify the following information:

url
The URL exposed by the Salesforce IoT Input Stream. The URL is available from the Salesforce IoT Platform when you create an Input Stream. Refer to the Salesforce IoT documentation to learn more.

token
The token used to authenticate access to the specified Salesforce IoT Input Stream. The token is available from the Salesforce IoT Platform when you create an Input Stream. Refer to the Salesforce IoT documentation to learn more.

Note
These parameters do not support substitution.

The following JSON example shows how to create an AWS IoT rule with a salesforce action:

```json
{
    "sql": "expression",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [{
        "salesforce": {
            "token": "ABCDEFGH123456789abcdefgh123456789",
            "url": "https://ingestion-cluster-id.my-env.sfdcnow.com/streams/stream-id/connection-id/my-event"
        }
    }]
}
```
For more information, refer to the Salesforce IoT documentation.

**SNS Action**

A `sns` action sends the data from the MQTT message that triggered the rule as an SNS push notification.

**more info (13)**

When creating a rule with an `sns` action, you must specify the following information:

- **messageFormat**
  The message format. Accepted values are "JSON" and "RAW." The default value of the attribute is "RAW." SNS uses this setting to determine if the payload should be parsed and relevant platform-specific parts of the payload should be extracted.

- **roleArn**
  The IAM role that allows access to SNS.

- **targetArn**
  The SNS topic or individual device to which the push notification is sent.

**Note**
Make sure the policy associated with the rule has the `sns:Publish` permission.

The following JSON example shows how to define an `sns` action in an AWS IoT rule:

```json
{
  "rule": {
    "sql": "SELECT * FROM 'some/topic'",
    "ruleDisabled": false,
    "actions": [{
      "sns": {
        "roleArn": "arn:aws:iam::123456789012:role/aws_iot_sns"
      }
    }
  ]
}
```

For more information, see the Amazon SNS Developer Guide.

**SQS Action**

A `sqs` action sends data from the MQTT message that triggered the rule to an SQS queue.

**more info (14)**

When creating a rule with an `sqs` action, you must specify the following information:
queueUrl

The URL of the SQS queue to which to write the data.

useBase64

Set to true if you want the MQTT message data to be Base64-encoded before writing to the SQS queue. Otherwise, set to false.

roleArn

The IAM role that allows access to the SQS queue.

Note

Make sure the role associated with the rule has a policy granting the sqs:SendMessage permission.

The following JSON example shows how to create an AWS IoT rule with an sqs action:

```json
{
  "rule": {
    "sql": "SELECT * FROM 'some/topic'",
    "ruleDisabled": false,
    "actions": [{
      "sqs": {
        "queueUrl": "https://sqs.us-east-2.amazonaws.com/123456789012/my_sqs_queue",
        "roleArn": "arn:aws:iam::123456789012:role/aws_iot_sqs",
        "useBase64": false
      }
    }
  }
}
```

For more information, see the Amazon SQS Developer Guide.

Step Functions Action

A stepFunctions action starts execution of a Step Functions state machine.

When creating a rule with a stepFunctions action, you must specify the following information:

executionNamePrefix

(Optional) A name will be given to the state machine execution consisting of this prefix followed by a UUID. Step Functions automatically creates a unique name for each state machine execution if one is not provided.

stateMachineName

The name of the Step Functions state machine whose execution will be started.

roleArn

The ARN of the role that grants IoT permission to start execution of a state machine ("Action":"states:StartExecution").

Here is an example trust policy that should be attached to the role:
AWS IoT SQL Reference

In AWS IoT, rules are defined using an SQL-like syntax. SQL statements are composed of three types of clauses:

**SELECT**
Required. Extracts information from the incoming payload and performs transformations.

**FROM**
Required. The MQTT topic filter from which the rule receives messages.

**WHERE**
Optional. Adds conditional logic that determines if a rule is evaluated and its actions are executed.

An example SQL statement looks like this:

```
SELECT color AS rgb FROM 'a/b' WHERE temperature > 50
```

An example MQTT message (also called an incoming payload) looks like this:

```
{
    "color":"red",
    "temperature":100
}
```
If this message is published on the 'a/b' topic, the rule is triggered and the SQL statement is evaluated. The SQL statement extracts the value of the color property if the "temperature" property is greater than 50. The WHERE clause specifies the condition temperature > 50. The AS keyword renames the "color" property to "rgb". The result (also called an outgoing payload) looks like this:

```json
{   "rgb":"red"
}
```

This data is then forwarded to the rule's action, which sends the data for more processing. For more information about rule actions, see AWS IoT Rule Actions (p. 186).

## Data Types

The AWS IoT rules engine supports all JSON data types.

### Supported Data Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>A discrete Int. 34 digits maximum.</td>
</tr>
<tr>
<td>Decimal</td>
<td>A Decimal with a precision of 34 digits, with a minimum non-zero magnitude of 1E-999 and a maximum magnitude 9.999...E999.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Some functions return Decimals with double precision rather than 34-digit precision.</td>
</tr>
<tr>
<td>Boolean</td>
<td>True or False.</td>
</tr>
<tr>
<td>String</td>
<td>A UTF-8 string.</td>
</tr>
<tr>
<td>Array</td>
<td>A series of values that don't have to have the same type.</td>
</tr>
<tr>
<td>Object</td>
<td>A JSON value consisting of a key and a value. Keys must be strings. Values can be any type.</td>
</tr>
<tr>
<td>Null</td>
<td>Null as defined by JSON. It's an actual value that represents the absence of a value. You can explicitly create a Null value by using the Null keyword in your SQL statement. For example: &quot;SELECT NULL AS n FROM 'a/b'&quot;</td>
</tr>
<tr>
<td>Undefined</td>
<td>Not a value. This isn't explicitly representable in JSON except by omitting the value. For example, in the object {&quot;foo&quot;: null}, the key &quot;foo&quot; returns NULL, but the key &quot;bar&quot; returns Undefined. Internally, the SQL language treats Undefined as a value, but it isn't representable in JSON, so when serialized to JSON, the results are Undefined.</td>
</tr>
</tbody>
</table>

```json
{"foo":null, "bar":undefined}
```

is serialized to JSON as:
Similarly, `Undefined` is converted to an empty string when serialized by itself. Functions called with invalid arguments (for example, wrong types, wrong number of arguments, and so on) return `Undefined`.

**Conversions**

The following table lists the results when a value of one type is converted to another type (when a value of the incorrect type is given to a function). For example, if the absolute value function "abs" (which expects an `Int` or `Decimal`) is given a `String`, it attempts to convert the `String` to a `Decimal`, following these rules. In this case, ‘abs("-5.123")’ is treated as ‘abs(-5.123)’.

**Note**

There are no attempted conversions to `Array`, `Object`, `Null`, or `Undefined`.

### To Decimal

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Int</code></td>
<td>A Decimal with no decimal point.</td>
</tr>
<tr>
<td><code>Decimal</code></td>
<td>The source value.</td>
</tr>
<tr>
<td><code>Boolean</code></td>
<td><code>Undefined</code>. (You can explicitly use the cast function to transform true = 1.0, false = 0.0.)</td>
</tr>
<tr>
<td><code>String</code></td>
<td>The SQL engine tries to parse the string as a Decimal. AWS IoT attempts to parse strings matching the regular expression: `^-?\d+(.\d+)?((?i)E-?\d+)?$. &quot;0&quot;, &quot;-1.2&quot;, &quot;5E-12&quot; are all examples of strings that would be automatically converted to Decimals.</td>
</tr>
<tr>
<td><code>Array</code></td>
<td><code>Undefined</code>.</td>
</tr>
<tr>
<td><code>Object</code></td>
<td><code>Undefined</code>.</td>
</tr>
<tr>
<td><code>Null</code></td>
<td><code>Null</code>.</td>
</tr>
<tr>
<td><code>Undefined</code></td>
<td><code>Undefined</code>.</td>
</tr>
</tbody>
</table>

### To Int

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Int</code></td>
<td>The source value.</td>
</tr>
<tr>
<td><code>Decimal</code></td>
<td>The source value rounded to the nearest <code>Int</code>.</td>
</tr>
<tr>
<td><code>Boolean</code></td>
<td><code>Undefined</code>. (You can explicitly use the cast function to transform true = 1.0, false = 0.0.)</td>
</tr>
</tbody>
</table>
AWS IoT Developer Guide
Data Types

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The SQL engine will try to parse the string as a Decimal. We will attempt to parse strings matching the regular expression: <code>^[-+]?\d+\.(\d+)?((?i)E[-+]?\d+)?</code>. &quot;0&quot;, &quot;-1.2&quot;, &quot;5E-12&quot; are all examples of strings that would automatically be converted to Decimals. We will attempt to convert the String to a Decimal, and then truncate the decimal places of that Decimal to make an Int.</td>
</tr>
<tr>
<td>Array</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Null.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**To Boolean**

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Undefined. (You can explicitly use the cast function to transform 0 = False, any_nonzero_value = True.)</td>
</tr>
<tr>
<td>Decimal</td>
<td>Undefined. (You can explicitly use the cast function to transform 0 = False, any_nonzero_value = True.)</td>
</tr>
<tr>
<td>Boolean</td>
<td>The original value.</td>
</tr>
<tr>
<td>String</td>
<td>&quot;true&quot;=True and &quot;false&quot;=False (case-insensitive). Other string values will be Undefined.</td>
</tr>
<tr>
<td>Array</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**To String**

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>A string representation of the Int in standard notation.</td>
</tr>
<tr>
<td>Decimal</td>
<td>A string representing the Decimal value, possibly in scientific notation.</td>
</tr>
<tr>
<td>Boolean</td>
<td>&quot;true&quot; or &quot;false&quot;. All lowercase.</td>
</tr>
<tr>
<td>String</td>
<td>The original value.</td>
</tr>
</tbody>
</table>
## Operators

The following operators can be used in SELECT, FROM, and WHERE clauses.

### AND operator

Returns a Boolean result. Performs a logical AND operation. Returns true if left and right operands are true. Otherwise, returns false. Boolean operands or case-insensitive "true" or "false" string operands are required.

**Syntax:** `expression AND expression`.

### AND Operator

<table>
<thead>
<tr>
<th>Left Operand</th>
<th>Right Operand</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean</td>
<td>Boolean</td>
<td>Boolean. True if both operands are true. Otherwise, false.</td>
</tr>
<tr>
<td>String/Boolean</td>
<td>String/Boolean</td>
<td>If all strings are &quot;true&quot; or &quot;false&quot; (case-insensitive), they are converted to Boolean and processed normally as <code>boolean AND boolean</code>.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Other Value</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

### OR operator

Returns a Boolean result. Performs a logical OR operation. Returns true if either the left or the right operands are true. Otherwise, returns false. Boolean operands or case-insensitive "true" or "false" string operands are required.

**Syntax:** `expression OR expression`.

### OR Operator

<table>
<thead>
<tr>
<th>Left Operand</th>
<th>Right Operand</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean</td>
<td>Boolean</td>
<td>Boolean. True if either operand is true. Otherwise, false.</td>
</tr>
<tr>
<td>Left Operand</td>
<td>Right Operand</td>
<td>Output</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>String/Boolean</td>
<td>String/Boolean</td>
<td>If all strings are &quot;true&quot; or &quot;false&quot; (case-insensitive), they are</td>
</tr>
<tr>
<td></td>
<td></td>
<td>converted to Booleans and processed normally as <strong>boolean</strong> OR <strong>boolean</strong>.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Other Value</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**NOT operator**

Returns a Boolean result. Performs a logical NOT operation. Returns true if the operand is false. Otherwise, returns true. A boolean operand or case-insensitive "true" or "false" string operand is required.

**Syntax:** `NOT expression`.

<table>
<thead>
<tr>
<th>Operand</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean</td>
<td>Boolean. True if operand is false. Otherwise, true.</td>
</tr>
<tr>
<td>String</td>
<td>If string is &quot;true&quot; or &quot;false&quot; (case-insensitive), it is</td>
</tr>
<tr>
<td></td>
<td>converted to the corresponding boolean value, and the opposite value is returned.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**> operator**

Returns a Boolean result. Returns true if the left operand is greater than the right operand. Both operands are converted to a Decimal, and then compared.

**Syntax:** `expression > expression`.

<table>
<thead>
<tr>
<th>Left Operand</th>
<th>Right Operand</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int/Decimal</td>
<td>Int/Decimal</td>
<td>Boolean. True if the left operand is greater than the right operand. Otherwise, false.</td>
</tr>
<tr>
<td>String/Int/Decimal</td>
<td>String/Int/Decimal</td>
<td>If all strings can be converted to Decimal, then Boolean. Returns true if the left operand is greater than the right operand. Otherwise, false.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Undefined.</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**>= operator**

Returns a Boolean result. Returns true if the left operand is greater than or equal to the right operand. Both operands are converted to a Decimal, and then compared.

**Syntax:** `expression >= expression`. 
### >= Operator

<table>
<thead>
<tr>
<th>Left Operand</th>
<th>Right Operand</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int/Decimal</td>
<td>Int/Decimal</td>
<td>Boolean. True if the left operand is greater than or equal to the right operand. Otherwise, false.</td>
</tr>
<tr>
<td>String/Int/Decimal</td>
<td>String/Int/Decimal</td>
<td>If all strings can be converted to Decimal, then Boolean. Returns true if the left operand is greater than or equal to the right operand. Otherwise, false.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**< operator**

Returns a Boolean result. Returns true if the left operand is less than the right operand. Both operands are converted to a Decimal, and then compared.

**Syntax:** `expression < expression`.

### < Operator

<table>
<thead>
<tr>
<th>Left Operand</th>
<th>Right Operand</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int/Decimal</td>
<td>Int/Decimal</td>
<td>Boolean. True if the left operand is less than the right operand. Otherwise, false.</td>
</tr>
<tr>
<td>String/Int/Decimal</td>
<td>String/Int/Decimal</td>
<td>If all strings can be converted to Decimal, then Boolean. Returns true if the left operand is less than the right operand. Otherwise, false.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**<= operator**

Returns a Boolean result. Returns true if the left operand is less than or equal to the right operand. Both operands are converted to a Decimal, and then compared.

**Syntax:** `expression <= expression`.

### >= Operator

<table>
<thead>
<tr>
<th>Left Operand</th>
<th>Right Operand</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int/Decimal</td>
<td>Int/Decimal</td>
<td>Boolean. True if the left operand is less than or equal to the right operand. Otherwise, false.</td>
</tr>
<tr>
<td>String/Int/Decimal</td>
<td>String/Int/Decimal</td>
<td>If all strings can be converted to Decimal, then Boolean. Returns true if the left operand is less than or equal to the right operand. Otherwise, false.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**<> operator**

Returns a Boolean result. Returns true if both left and right operands are not equal. Otherwise, returns false.
### Operators

**Syntax:** `expression <> expression`.

**<> Operator**

<table>
<thead>
<tr>
<th>Left Operand</th>
<th>Right Operand</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Int</td>
<td>True if left operand is not equal to right operand. Otherwise, false.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Decimal</td>
<td>True if left operand is not equal to right operand. Otherwise, false. Int is converted to Decimal before being compared.</td>
</tr>
<tr>
<td>String</td>
<td>String</td>
<td>True if left operand is not equal to right operand. Otherwise, false.</td>
</tr>
<tr>
<td>Array</td>
<td>Array</td>
<td>True if the items in each operand are not equal and not in the same order. Otherwise, false.</td>
</tr>
<tr>
<td>Object</td>
<td>Object</td>
<td>True if the keys and values of each operand are not equal. Otherwise, false. The order of keys/values is unimportant.</td>
</tr>
<tr>
<td>Null</td>
<td>Null</td>
<td>False.</td>
</tr>
<tr>
<td>Any Value</td>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Any Value</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Mismatched Type</td>
<td>Mismatched Type</td>
<td>True.</td>
</tr>
</tbody>
</table>

**= operator**

Returns a Boolean result. Returns true if both left and right operands are equal. Otherwise, returns false.

**Syntax:** `expression = expression`.

**= Operator**

<table>
<thead>
<tr>
<th>Left Operand</th>
<th>Right Operand</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Int</td>
<td>True if left operand is equal to right operand. Otherwise, false.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Decimal</td>
<td>True if left operand is equal to right operand. Otherwise, false. Int is converted to Decimal before being compared.</td>
</tr>
<tr>
<td>String</td>
<td>String</td>
<td>True if left operand is equal to right operand. Otherwise, false.</td>
</tr>
<tr>
<td>Array</td>
<td>Array</td>
<td>True if the items in each operand are equal and in the same order. Otherwise, false.</td>
</tr>
<tr>
<td>Object</td>
<td>Object</td>
<td>True if the keys and values of each operand are equal. Otherwise, false. The order of keys/values is unimportant.</td>
</tr>
<tr>
<td>Any Value</td>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Any Value</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Mismatched Type</td>
<td>Mismatched Type</td>
<td>False.</td>
</tr>
</tbody>
</table>
+ operator

The "+" is an overloaded operator. It can be used for string concatenation or addition.

Syntax: `expression + expression`.

<table>
<thead>
<tr>
<th>+ Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Left Operand</strong></td>
</tr>
<tr>
<td>------------------------------------------</td>
</tr>
<tr>
<td>String</td>
</tr>
<tr>
<td>Any Value</td>
</tr>
<tr>
<td>Int</td>
</tr>
<tr>
<td>Int/Decimal</td>
</tr>
<tr>
<td>Other Value</td>
</tr>
</tbody>
</table>

- operator

Subtracts the right operand from the left operand.

Syntax: `expression - expression`.

<table>
<thead>
<tr>
<th>- Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Left Operand</strong></td>
</tr>
<tr>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Int</td>
</tr>
<tr>
<td>Int/Decimal</td>
</tr>
<tr>
<td>String/Int/Decimal</td>
</tr>
<tr>
<td>Other Value</td>
</tr>
<tr>
<td>Other Value</td>
</tr>
</tbody>
</table>

* operator

Multiplies the left operand by the right operand.

Syntax: `expression * expression`.

<table>
<thead>
<tr>
<th>* Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Left Operand</strong></td>
</tr>
<tr>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Int</td>
</tr>
</tbody>
</table>
You can use the following built-in functions in the SELECT or WHERE clauses of your SQL expressions.

### Functions

**/ operator**

Divides the left operand by the right operand.

**Syntax:** `expression / expression`.

**% operator**

Returns the remainder from dividing the left operand by the right operand.

**Syntax:** `expression % expression`.

### / Operator

<table>
<thead>
<tr>
<th>Left Operand</th>
<th>Right Operand</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int/Decimal</td>
<td>Int/Decimal</td>
<td>Decimal value. Multiplies the left operand by the right operand.</td>
</tr>
<tr>
<td>String/Int/Decimal</td>
<td>String/Int/Decimal</td>
<td>If all strings convert to Decimals correctly, a Decimal value is returned. Multiplies the left operand by the right operand. Otherwise, returns Undefined.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Other value</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

### % Operator

<table>
<thead>
<tr>
<th>Left Operand</th>
<th>Right Operand</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Int</td>
<td>Int value. Divides the left operand by the right operand.</td>
</tr>
<tr>
<td>Int/Decimal</td>
<td>Int/Decimal</td>
<td>Decimal value. Divides the left operand by the right operand.</td>
</tr>
<tr>
<td>String/Int/Decimal</td>
<td>String/Int/Decimal</td>
<td>If all strings convert to Decimals correctly, a Decimal value is returned. Divides the left operand by the right operand. Otherwise, returns Undefined.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Other value</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>
abs(Decimal)

Returns the absolute value of a number. Supported by SQL version 2015-10-8 and later.

Example: abs(-5) returns 5.

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Int, the absolute value of the argument.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Decimal, the absolute value of the argument.</td>
</tr>
<tr>
<td>Boolean</td>
<td>Undefined.</td>
</tr>
<tr>
<td>String</td>
<td>Decimal. The result is the absolute value of the argument. If the string cannot be converted, the result is Undefined.</td>
</tr>
<tr>
<td>Array</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

accountid()

Returns the ID of the account that owns this rule as a String. Supported by SQL version 2015-10-8 and later.

Example:

accountid() = "123456789012"

acos(Decimal)

Returns the inverse cosine of a number in radians. Decimal arguments are rounded to double precision before function application. Supported by SQL version 2015-10-8 and later.

Example: acos(0) = 1.5707963267948966

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Decimal (with double precision), the inverse cosine of the argument. Imaginary results are returned as Undefined.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Decimal (with double precision), the inverse cosine of the argument. Imaginary results are returned as Undefined.</td>
</tr>
<tr>
<td>Boolean</td>
<td>Undefined.</td>
</tr>
<tr>
<td>String</td>
<td>Decimal, the inverse cosine of the argument. If the string cannot be converted, the result is Undefined. Imaginary results are returned as Undefined.</td>
</tr>
</tbody>
</table>
### Argument Type | Result
---|---
Array | Undefined.
Object | Undefined.
Null | Undefined.
Undefined | Undefined.

#### asin(Decimal)

Returns the inverse sine of a number in radians. Decimal arguments are rounded to double precision before function application. Supported by SQL version 2015-10-8 and later.

Example: \( \text{asin}(0) = 0.0 \)

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Decimal (with double precision), the inverse sine of the argument. Imaginary results are returned as Undefined.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Decimal (with double precision), the inverse sine of the argument. Imaginary results are returned as Undefined.</td>
</tr>
<tr>
<td>Boolean</td>
<td>Undefined.</td>
</tr>
<tr>
<td>String</td>
<td>Decimal (with double precision), the inverse sine of the argument. If the string cannot be converted, the result is Undefined. Imaginary results are returned as Undefined.</td>
</tr>
<tr>
<td>Array</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

#### atan(Decimal)

Returns the inverse tangent of a number in radians. Decimal arguments are rounded to double precision before function application. Supported by SQL version 2015-10-8 and later.

Example: \( \text{atan}(0) = 0.0 \)

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Decimal (with double precision), the inverse tangent of the argument. Imaginary results are returned as Undefined.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Decimal (with double precision), the inverse tangent of the argument. Imaginary results are returned as Undefined.</td>
</tr>
<tr>
<td>Argument Type</td>
<td>Result</td>
</tr>
<tr>
<td>---------------</td>
<td>--------</td>
</tr>
<tr>
<td>Boolean</td>
<td>Undefined.</td>
</tr>
<tr>
<td>String</td>
<td>Decimal, the inverse tangent of the argument. If the string cannot be converted, the result is Undefined. Imaginary results are returned as Undefined.</td>
</tr>
<tr>
<td>Array</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**atan2(Decimal, Decimal)**

Returns the angle, in radians, between the positive x-axis and the (x, y) point defined in the two arguments. The angle is positive for counter-clockwise angles (upper half-plane, y > 0), and negative for clockwise angles (lower half-plane, y < 0). Decimal arguments are rounded to double precision before function application. Supported by SQL version 2015-10-8 and later.

Example: \( \text{atan2}(1, 0) = 1.5707963267948966 \)

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int/Decimal</td>
<td>Int/Decimal</td>
<td>Decimal (with double x-axis and the specified y-axis)</td>
</tr>
<tr>
<td>Int/Decimal/String</td>
<td>Int/Decimal/String</td>
<td>Decimal, the inverse tangent of the point described. If a string cannot be converted, the result is Undefined.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Other Value</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**aws_lambda(functionArn, inputJson)**

Calls the specified Lambda function passing `inputJson` to the Lambda function and returns the JSON generated by the Lambda function.

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>functionArn</td>
<td>The ARN of the Lambda function to call. The Lambda function must return JSON data.</td>
</tr>
<tr>
<td>inputJson</td>
<td>The JSON input passed to the Lambda function.</td>
</tr>
</tbody>
</table>

You must grant AWS IoT lambda:InvokeFunction permissions to invoke the specified Lambda function. The following example shows how to grant the lambda:InvokeFunction permission using the AWS CLI:

```
aws lambda add-permission --function-name "function_name" --region "region"
```
The following are the arguments for the add-permission command:

--function-name

Name of the Lambda function whose resource policy you are updating by adding a new permission.

--region

The AWS region of your account.

--principal

The principal who is getting the permission. This should be `iot.amazonaws.com` to allow AWS IoT permission to call a Lambda function.

--source-arn

The ARN of the rule. You can use the `get-topic-rule` CLI command to get the ARN of a rule.

--source-account

The AWS account where the rule is defined.

--statement-id

A unique statement identifier.

--action

The Lambda action you want to allow in this statement. In this case, we want to allow AWS IoT to invoke a Lambda function, so we specify `lambda:InvokeFunction`.

Note
If you add a permission for an AWS IoT principal without providing the source ARN, any AWS account that creates a rule with your Lambda action can trigger rules to invoke your Lambda function from AWS IoT.

For more information, see Lambda Permission Model.

The following rule shows how to call the `aws_lambda` function:

```sql
SELECT aws_lambda("arn:aws:lambda:us-east-1:account_id:function:lambda_function",
    payload.inner.element).some.value as output FROM 'a/b'
```

`payload.inner.element` selects data from message published on topic `a/b`.

`some.value` selects data from the output that is generated by the Lambda function.

Note
Rules Engine limits the execution duration of Lambda Functions. Lambda function calls from rules should be completed within 2000ms.

bitand(Int, Int)

Performs a bitwise AND on the bit representations of the two Int(-converted) arguments. Supported by SQL version 2015-10-8 and later.

Example: `bitand(13, 5) = 5`
### bitor(Int, Int)

Performs a bitwise OR of the bit representations of the two arguments. Supported by SQL version 2015-10-8 and later.

Example: bitor(8, 5) = 13

### bitxor(Int, Int)

Performs a bitwise XOR on the bit representations of the two Int(-converted) arguments. Supported by SQL version 2015-10-8 and later.

Example: bitxor(13, 5) = 8
### bitnot(Int)

Performs a bitwise NOT on the bit representations of the `Int(-converted)` argument. Supported by SQL version 2015-10-8 and later.

**Example:** `bitnot(13) = 2`

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Int, a bitwise NOT of the argument.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Int, a bitwise NOT of the argument. The Decimal value is rounded down to the nearest Int.</td>
</tr>
<tr>
<td>String</td>
<td>Int, a bitwise NOT of the argument. Strings are converted to Decimals and rounded down to the nearest Int. If any conversion fails, the result is Undefined.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Other value.</td>
</tr>
</tbody>
</table>

### cast()

Converts a value from one data type to another. Cast behaves mostly like the standard conversions, with the addition of the ability to cast numbers to/from `Boolean`es. If AWS IoT cannot determine how to cast one type to another, the result is Undefined. Supported by SQL version 2015-10-8 and later. Format: `cast(value as type)`.

**Example:**

```
cast(true as Decimal) = 1.0
```

The following keywords may appear after "as" when calling `cast`:

**For SQL version 2015-10-8 and 2016-03-23**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decimal</td>
<td>Casts value to Decimal.</td>
</tr>
<tr>
<td>Bool</td>
<td>Casts value to Boolean.</td>
</tr>
<tr>
<td>Boolean</td>
<td>Casts value to Boolean.</td>
</tr>
<tr>
<td>String</td>
<td>Casts value to String.</td>
</tr>
<tr>
<td>Nvarchar</td>
<td>Casts value to String.</td>
</tr>
<tr>
<td>Text</td>
<td>Casts value to String.</td>
</tr>
<tr>
<td>Ntext</td>
<td>Casts value to String.</td>
</tr>
<tr>
<td>varchar</td>
<td>Casts value to String.</td>
</tr>
<tr>
<td>Int</td>
<td>Casts value to Int.</td>
</tr>
</tbody>
</table>
### AWS IoT Developer Guide

**Functions**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integer</td>
<td>Casts value to Int.</td>
</tr>
</tbody>
</table>

**Additionally, for SQL version 2016-03-23**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decimal</td>
<td>Casts value to Decimal.</td>
</tr>
<tr>
<td>Bool</td>
<td>Casts value to Boolean.</td>
</tr>
<tr>
<td>Boolean</td>
<td>Casts value to Boolean.</td>
</tr>
</tbody>
</table>

Casting rules:

**Cast to Decimal**

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>A Decimal with no decimal point.</td>
</tr>
<tr>
<td>Decimal</td>
<td>The source value.</td>
</tr>
<tr>
<td>Boolean</td>
<td>true = 1.0, false = 0.0.</td>
</tr>
<tr>
<td>String</td>
<td>Will try to parse the string as a Decimal. We will attempt to parse strings matching the regex: ^-?\d+(\d+)?(?i)E-?\d+$&quot;. &quot;0&quot;, &quot;.-1.2&quot;, &quot;5E-12&quot; are all examples of Strings that would be converted automatically to Decimals.</td>
</tr>
<tr>
<td>Array</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**Cast to Int**

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>The source value.</td>
</tr>
<tr>
<td>Decimal</td>
<td>The source value, rounded down to the nearest Int.</td>
</tr>
<tr>
<td>Boolean</td>
<td>true = 1.0, false = 0.0.</td>
</tr>
<tr>
<td>String</td>
<td>Will try to parse the string as a Decimal. We will attempt to parse strings matching the regex: ^-?\d+(\d+)?(?i)E-?\d+$&quot;. &quot;0&quot;, &quot;.-1.2&quot;, &quot;5E-12&quot; are all examples of Strings that would be converted automatically to Decimals. Will attempt to convert the string to a Decimal and round down to the nearest Int.</td>
</tr>
<tr>
<td>Array</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>
### Argument Type vs. Result

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

### Cast to Boolean

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>0 = False, any_nonzero_value = True.</td>
</tr>
<tr>
<td>Decimal</td>
<td>0 = False, any_nonzero_value = True.</td>
</tr>
<tr>
<td>Boolean</td>
<td>The source value.</td>
</tr>
<tr>
<td>String</td>
<td>&quot;true&quot; = True and &quot;false&quot; = False (case-insensitive). Other string values = Undefined.</td>
</tr>
<tr>
<td>Array</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

### Cast to String

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>A string representation of the Int, in standard notation.</td>
</tr>
<tr>
<td>Decimal</td>
<td>A string representing the Decimal value, possibly in scientific notation.</td>
</tr>
<tr>
<td>Boolean</td>
<td>&quot;true&quot; or &quot;false&quot;, all lowercase.</td>
</tr>
<tr>
<td>String</td>
<td>&quot;true&quot;=True and &quot;false&quot;=False (case-insensitive). Other string values = Undefined.</td>
</tr>
<tr>
<td>Array</td>
<td>The array serialized to JSON. The result string will be a comma-separated list enclosed in square brackets. Strings are quoted. Decimals, Ints, Booleans are not.</td>
</tr>
<tr>
<td>Object</td>
<td>The object serialized to JSON. The JSON string will be a comma-separated list of key-value pairs and will begin and end with curly braces. Strings are quoted. Decimals, Ints, Booleans and Null are not.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>
ceil(Decimal)

Rounds the given Decimal up to the nearest Int. Supported by SQL version 2015-10-8 and later.

Examples:

\[
\text{ceil}(1.2) = 2 \\
\text{ceil}(11.2) = -1
\]

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Int, the argument value.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Int, the Decimal value rounded up to the nearest Int.</td>
</tr>
<tr>
<td>String</td>
<td>Int. The string is converted to Decimal and rounded up to the nearest Int. If the string cannot be converted to a Decimal, the result is Undefined.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

chr(String)

Returns the ASCII character that corresponds to the given Int argument. Supported by SQL version 2015-10-8 and later.

Examples:

\[
\text{chr}(65) = "A". \\
\text{chr}(49) = "1".
\]

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>The character corresponding to the specified ASCII value. If the argument is not a valid ASCII value, the result is Undefined.</td>
</tr>
<tr>
<td>Decimal</td>
<td>The character corresponding to the specified ASCII value. The Decimal argument is rounded down to the nearest Int. If the argument is not a valid ASCII value, the result is Undefined.</td>
</tr>
<tr>
<td>Boolean</td>
<td>Undefined.</td>
</tr>
<tr>
<td>String</td>
<td>If the String can be converted to a Decimal, it is rounded down to the nearest Int. If the argument is not a valid ASCII value, the result is Undefined.</td>
</tr>
<tr>
<td>Array</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>
**clientid()**

Returns the ID of the MQTT client sending the message, or n/a if the message wasn't sent over MQTT. Supported by SQL version 2015-10-8 and later.

Example:

```sql
clientid() = "123456789012"
```

**concat()**

Concatenates arrays or strings. This function accepts any number of arguments and returns a String or an Array. Supported by SQL version 2015-10-8 and later.

Examples:

```sql
concat() = Undefined.
concat(1) = "1".
concat([1, 2, 3], 4) = [1, 2, 3, 4].
concat([1, 2, 3], "hello") = [1, 2, 3,"hello"]
concat("con", "cat") = "concat"
concat(1, "hello") = "1hello"
concat("he","is","man") = "heisman"
concat([1, 2, 3], "hello", [4, 5, 6]) = [1, 2, 3, "hello", 4, 5, 6]
```

<table>
<thead>
<tr>
<th>Number of Arguments</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Undefined.</td>
</tr>
<tr>
<td>1</td>
<td>The argument is returned unmodified.</td>
</tr>
<tr>
<td>2+</td>
<td>If any argument is an Array, the result is a single array containing all of the arguments. If no arguments are Arrays, and at least one argument is a String, the result is the concatenation of the String representations of all the arguments. Arguments will be converted to Strings using the standard conversions listed above.</td>
</tr>
</tbody>
</table>

**cos(Decimal)**

Returns the cosine of a number in radians. Decimal arguments are rounded to double precision before function application. Supported by SQL version 2015-10-8 and later.

Example:

```sql
cos(0) = 1.
```

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Decimal (with double precision), the cosine of the argument. Imaginary results are returned as Undefined.</td>
</tr>
<tr>
<td>Argument Type</td>
<td>Result</td>
</tr>
<tr>
<td>---------------</td>
<td>--------</td>
</tr>
<tr>
<td>Decimal</td>
<td>Decimal (with double precision), the cosine of the argument. Imaginary results are returned as Undefined.</td>
</tr>
<tr>
<td>Boolean</td>
<td>Undefined.</td>
</tr>
<tr>
<td>String</td>
<td>Decimal (with double precision), the cosine of the argument. If the string cannot be converted to a Decimal, the result is Undefined. Imaginary results are returned as Undefined.</td>
</tr>
<tr>
<td>Array</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**cosh(Decimal)**

Returns the hyperbolic cosine of a number in radians. Decimal arguments are rounded to double precision before function application. Supported by SQL version 2015-10-8 and later.

Example: `cosh(2.3) = 5.037220649268761`.

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Decimal (with double precision), the hyperbolic cosine of the argument. Imaginary results are returned as Undefined.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Decimal (with double precision), the hyperbolic cosine of the argument. Imaginary results are returned as Undefined.</td>
</tr>
<tr>
<td>Boolean</td>
<td>Undefined.</td>
</tr>
<tr>
<td>String</td>
<td>Decimal (with double precision), the hyperbolic cosine of the argument. If the string cannot be converted to a Decimal, the result is Undefined. Imaginary results are returned as Undefined.</td>
</tr>
<tr>
<td>Array</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**encode(value, encodingScheme)**

Use the `encode` function to encode the payload, which potentially might be non-JSON data, into its string representation based on the encoding scheme. Supported by SQL version 2016-03-23 and later.
value

Any of the valid expressions, as defined in AWS IoT SQL Reference (p. 200). In addition, you can specify * to encode the entire payload, regardless of whether it's in JSON format. If you supply an expression, the result of the evaluation will first be converted to a string before it is encoded.

encodingScheme

A literal string representing the encoding scheme you want to use. Currently, only 'base64' is supported.

endswith(String, String)

Returns a Boolean indicating whether the first String argument ends with the second String argument. If either argument is Null or Undefined, the result is Undefined. Supported by SQL version 2015-10-8 and later.

Example: endswith("cat","at") = true.

<table>
<thead>
<tr>
<th>argument Type 1</th>
<th>argument Type 2</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>String</td>
<td>True if the first argument ends in the second argument. Otherwise, false.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Other Value</td>
<td>Both arguments are converted to Strings using the standard conversion rules. True if the first argument ends in the second argument. Otherwise, false. If either argument is Null or Undefined, the result is Undefined.</td>
</tr>
</tbody>
</table>

exp(Decimal)

Returns e raised to the Decimal argument. Decimal arguments are rounded to double precision before function application. Supported by SQL version 2015-10-8 and later.

Example: exp(1) = e.

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Decimal (with double precision), e ^ argument.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Decimal (with double precision), e ^ argument.</td>
</tr>
<tr>
<td>String</td>
<td>Decimal (with double precision), e ^ argument. If the String cannot be converted to a Decimal, the result is Undefined.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

get

Extracts a value from a collection-like type (Array, String, Object). No conversion will be applied to the first argument. Conversion applies as documented in the table to the second argument. Supported by SQL version 2015-10-8 and later.
Examples:

get(["a", "b", "c"], 1) = "b"
get({"a":"b"}, "a") = "b"
get("abc", 1) = "b"

<table>
<thead>
<tr>
<th>argument Type 1</th>
<th>argument Type 2</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Array</td>
<td>Any Type (converted to Int)</td>
<td>The item at the 0-based index of the Array provided by the second argument (converted to Int). If the conversion is unsuccessful, the result is Undefined. If the index is outside the bounds of the Array (negative or &gt;= array.length), the result is Undefined.</td>
</tr>
<tr>
<td>String</td>
<td>Any Type (converted to Int)</td>
<td>The character at the 0-based index of the string provided by the second argument (converted to Int). If the conversion is unsuccessful, the result is Undefined. If the index is outside the bounds of the string (negative or &gt;= string.length), the result is Undefined.</td>
</tr>
<tr>
<td>Object</td>
<td>String (no conversion is applied)</td>
<td>The value stored in the first argument object corresponding to the string key provided as the second argument.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Any Value</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

get_thing_shadow(thingName, roleARN)

Returns the shadow of the specified thing. Supported by SQL version 2016-03-23 and later.

thingName

String: The name of the thing whose shadow you want to retrieve.

roleArn

String: A role ARN with iot:GetThingShadow permission.

Example:

SELECT * from 'a/b'
WHERE get_thing_shadow("MyThing","arn:aws:iam::123456789012:role/AllowsThingShadowAccess") .state.reported.alarm = 'ON'

Hashing Functions

AWS IoT provides the following hashing functions:

- md2
- md5
- sha1
- sha224
- sha256
- sha384
• sha512

All hash functions expect one string argument. The result is the hashed value of that string. Standard string conversions apply to non-string arguments. All hash functions are supported by SQL version 2015-10-8 and later.

Examples:

\[ \text{md2("hello") = "a9046c73e00331af68917d3804f70655"} \]
\[ \text{md5("hello") = "5d41402abc4b2a76b9719d911017c592"} \]

**indexOf(String, String)**

Returns the first index (0-based) of the second argument as a substring in the first argument. Both arguments are expected as strings. Arguments that are not strings are subjected to standard string conversion rules. This function does not apply to arrays, only to strings. Supported by SQL version 2015-10-8 and later.

Examples:

\[ \text{indexOf("abcd", "bc") = 1} \]

**isNull()**

Returns whether the argument is the Null value. Supported by SQL version 2015-10-8 and later.

Examples:

\[ \text{isNull(5) = false.} \]
\[ \text{isNull(Null) = true.} \]

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>false</td>
</tr>
<tr>
<td>Decimal</td>
<td>false</td>
</tr>
<tr>
<td>Boolean</td>
<td>false</td>
</tr>
<tr>
<td>String</td>
<td>false</td>
</tr>
<tr>
<td>Array</td>
<td>false</td>
</tr>
<tr>
<td>Object</td>
<td>false</td>
</tr>
<tr>
<td>Null</td>
<td>true</td>
</tr>
<tr>
<td>Undefined</td>
<td>false</td>
</tr>
</tbody>
</table>

**isUndefined()**

Returns whether the argument is Undefined. Supported by SQL version 2015-10-8 and later.

Examples:

\[ \text{isUndefined(5) = false.} \]
isNull(floor([1,2,3]))) = true.

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>false</td>
</tr>
<tr>
<td>Decimal</td>
<td>false</td>
</tr>
<tr>
<td>Boolean</td>
<td>false</td>
</tr>
<tr>
<td>String</td>
<td>false</td>
</tr>
<tr>
<td>Array</td>
<td>false</td>
</tr>
<tr>
<td>Object</td>
<td>false</td>
</tr>
<tr>
<td>Null</td>
<td>false</td>
</tr>
<tr>
<td>Undefined</td>
<td>true</td>
</tr>
</tbody>
</table>

**length(String)**

Returns the number of characters in the provided string. Standard conversion rules apply to non-String arguments. Supported by SQL version 2015-10-8 and later.

Examples:

\[
\text{length("hi") = 2}
\]

\[
\text{length(false) = 5}
\]

**ln(Decimal)**

Returns the natural logarithm of the argument. Decimal arguments are rounded to double precision before function application. Supported by SQL version 2015-10-8 and later.

Example: \(\ln(e) = 1\).
**log(Decimal)**

Returns the base 10 logarithm of the argument. Decimal arguments are rounded to double precision before function application. Supported by SQL version 2015-10-8 and later.

Example: \( \log(100) = 2.0 \).

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Decimal (with double precision), the base 10 log of the argument.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Decimal (with double precision), the base 10 log of the argument.</td>
</tr>
<tr>
<td>Boolean</td>
<td>Undefined.</td>
</tr>
<tr>
<td>String</td>
<td>Decimal (with double precision), the base 10 log of the argument. If the String cannot be converted to a Decimal, the result is Undefined.</td>
</tr>
<tr>
<td>Array</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**lower(String)**

Returns the lowercase version of the given String. Non-string arguments are converted to Strings using the standard conversion rules. Supported by SQL version 2015-10-8 and later.

Examples:

lower("HELLO") = "hello".

lower(["HELLO"]) = 
["hello"].

**lpad(String, Int)**

Returns the String argument, padded on the left side with the number of spaces specified by the second argument. The Int argument must be between 0 and 1000. If the provided value is outside of this valid range, the argument will be set to the nearest valid value (0 or 1000). Supported by SQL version 2015-10-8 and later.

Examples:

lpad("hello", 2) = "hello".

lpad(1, 3) = " 1"
### Functions

<table>
<thead>
<tr>
<th>argument Type 1</th>
<th>argument Type 2</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>Decimal</td>
<td>The Decimal argument will be rounded down to the nearest Int and the String is padded on the left with the specified number of spaces.</td>
</tr>
<tr>
<td>String</td>
<td>String</td>
<td>The second argument is converted to a Decimal, which is rounded down to the nearest Int, and the String is padded with the specified number of spaces on the left. If the second argument cannot be converted to an Int, the result is Undefined.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Int/Decimal/String</td>
<td>The first value will be converted to a String using the standard conversions, and then the LPAD function will be applied on that String. If it cannot be converted, the result is Undefined.</td>
</tr>
<tr>
<td>Any Value</td>
<td>Other Value</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**ltrim(String)**

Removes all leading whitespace (tabs and spaces) from the provided String. Supported by SQL version 2015-10-8 and later.

Example:

```
ltrim(" h i ") = "hi".
```

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>The String representation of the Int with all leading whitespace removed.</td>
</tr>
<tr>
<td>Decimal</td>
<td>The String representation of the Decimal with all leading whitespace removed.</td>
</tr>
<tr>
<td>Boolean</td>
<td>The String representation of the boolean (&quot;true&quot; or &quot;false&quot;) with all leading whitespace removed.</td>
</tr>
<tr>
<td>String</td>
<td>The argument with all leading whitespace removed.</td>
</tr>
<tr>
<td>Array</td>
<td>The String representation of the Array (using standard conversion rules) with all leading whitespace removed.</td>
</tr>
<tr>
<td>Object</td>
<td>The String representation of the Object (using standard conversion rules) with all leading whitespace removed.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**machinelearning_predict(modelId)**

Use the `machinelearning_predict` function to make predictions using the data from an MQTT message based on an Amazon Machine Learning (Amazon ML) model. Supported by SQL version 2015-10-8 and later. The arguments for the `machinelearning_predict` function are:
modelId

The ID of the model against which to run the prediction. The real-time endpoint of the model must be enabled.

roleArn

The IAM role that has a policy with machinelearning:Predict and machinelearning:GetMLModel permissions and allows access to the model against which the prediction is run.

record

The data to be passed into the Amazon ML Predict API. This should be represented as a single layer JSON object. If the record is a multi-level JSON object, the record will be flattened by serializing its values. For example, the following JSON:

{ "key1": {"innerKey1": "value1"}, "key2": 0 }

would become:

{ "key1": "{"innerKey1": "value1""}, "key2": 0 }

The function returns a JSON object with the following fields:

predictedLabel

The classification of the input based on the model.

details

Contains the following attributes:

PredictiveModelType

The model type. Valid values are REGRESSION, BINARY, MULTICLASS.

Algorithm

The algorithm used by Amazon ML to make predictions. The value must be SGD.

predictedScores

Contains the raw classification score corresponding to each label.

predictedValue

The value predicted by Amazon ML.

**mod(Decimal, Decimal)**

Returns the remainder of the division of the first argument by the second argument. Supported by SQL version 2015-10-8 and later. You can also use "%" as an infix operator for the same modulo functionality. Supported by SQL version 2015-10-8 and later.

Example: \( \text{mod}(8, 3) = 2 \).

<table>
<thead>
<tr>
<th>Left Operand</th>
<th>Right Operand</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Int</td>
<td>Int, the first argument</td>
</tr>
<tr>
<td>Int/Decimal</td>
<td>Int/Decimal</td>
<td>Decimal, the first argument</td>
</tr>
</tbody>
</table>
### nanvl(AnyValue, AnyValue)

Returns the first argument if it is a valid Decimal. Otherwise, the second argument is returned. Supported by SQL version 2015-10-8 and later.

Example: `Nanvl(8, 3) = 8`.

<table>
<thead>
<tr>
<th>argument Type 1</th>
<th>argument Type 2</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undefined</td>
<td>Any Value</td>
<td>The second argument.</td>
</tr>
<tr>
<td>Null</td>
<td>Any Value</td>
<td>The second argument.</td>
</tr>
<tr>
<td>Decimal (NaN)</td>
<td>Any Value</td>
<td>The second argument.</td>
</tr>
<tr>
<td>Decimal (not NaN)</td>
<td>Any Value</td>
<td>The first argument.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Any Value</td>
<td>The first argument.</td>
</tr>
</tbody>
</table>

### newuuid()

Returns a random 16-byte UUID. Supported by SQL version 2015-10-8 and later.

Example: `newuuid() = 123a4567-b89c-12d3-e456-789012345000`

### numbytes(String)

Returns the number of bytes in the UTF-8 encoding of the provided string. Standard conversion rules apply to non-String arguments. Supported by SQL version 2015-10-8 and later.

Examples:

- `numbytes("hi") = 2`
- `numbytes("€") = 3`

### principal()

Returns the X.509 certificate fingerprint or thing name, depending on which endpoint, MQTT or HTTP, received the request. Supported by SQL version 2015-10-8 and later.

Example:

- `principal() = "ba67293af50bf2506f5f93469686da660c7c844e7b3950bfb16813e0d31e9373"

### parse_time(String, Long, [String])

Use the `parse_time` function to format a timestamp into a human-readable date/time format. Supported by SQL version 2016-03-23 and later. The arguments for the `parse_time` function are:
pattern

(String) A date/time pattern which conforms to the ISO 8601 standard format. (Specifically, the function supports Joda-Time formats.)

timestamp

(Long) The time to be formatted in milliseconds since Unix epoch. See function timestamp() (p. 240).

timezone

(String) [Optional] The time zone of the formatted date/time. The default is "UTC". The function supports Joda-Time time zones.

Examples:

When this message is published to the topic 'A/B', the payload {"ts": "1970.01.01 AD at 21:46:40 CST"} will be sent to the S3 bucket:

```json
{
    "rule": {
        "awsIotSqlVersion": "2016-03-23",
        "sql": "SELECT parse_time("yyyy.MM.dd G 'at' HH:mm:ss z", 100000000, "America/Belize") as ts FROM 'A/B'",
        "ruleDisabled": false,
        "actions": [
            {
                "s3": {
                    "roleArn": "arn:aws:iam::ACCOUNT_ID:rule:role/ROLE_NAME",
                    "bucketName": "BUCKET_NAME",
                    "key": "KEY_NAME"
                }
            }
        ],
        "ruleName": "RULE_NAME"
    }
}
```

When this message is published to the topic 'A/B', a payload similar to {"ts": "2017.06.09 AD at 17:19:46 UTC"} (but with the current date/time) will be sent to the S3 bucket:

```json
{
    "rule": {
        "awsIotSqlVersion": "2016-03-23",
        "sql": "SELECT parse_time("yyyy.MM.dd G 'at' HH:mm:ss z", timestamp()) as ts FROM 'A/B'",
        "ruleDisabled": false,
        "actions": [
            {
                "s3": {
                    "roleArn": "arn:aws:iam::ACCOUNT_ID:rule:role/ROLE_NAME",
                    "bucketName": "BUCKET_NAME",
                    "key": "KEY_NAME"
                }
            }
        ],
        "ruleName": "RULE_NAME"
    }
}
```
parse_time() can also be used as a substitution template. For example, when this message is published to the topic 'A/B', the payload will be sent to the S3 bucket with key = "2017":

```json
{
    "rule": {
        "awsIotSqlVersion": "2016-03-23",
        "sql": "SELECT * FROM 'A/B'",
        "ruleDisabled": false,
        "actions": [
            {
                "s3": {
                    "roleArn": "arn:aws:iam::ACCOUNT_ID:rule:role/ROLE_NAME",
                    "bucketName": BUCKET_NAME,
                    "key": "${parse_time("yyyy", timestamp(), "UTC")}"}]
            }
        
    },
    "ruleName": "RULE_NAME"
}
```

**power(Decimal, Decimal)**

Returns the first argument raised to the second argument. Decimal arguments are rounded to double precision before function application. Supported by SQL version 2015-10-8 and later. Supported by SQL version 2015-10-8 and later.

Example: `power(2, 5) = 32.0`.

<table>
<thead>
<tr>
<th>argument Type 1</th>
<th>argument Type 2</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int/Decimal</td>
<td>Int/Decimal</td>
<td>A Decimal (with double precision), the first argument raised to the second argument's power.</td>
</tr>
<tr>
<td>Int/Decimal/String</td>
<td>Int/Decimal/String</td>
<td>A Decimal (with double precision), the first argument raised to the second argument's power. Any strings are converted to Decimals. If any String fails to be converted to Decimal, the result is Undefined.</td>
</tr>
<tr>
<td>Other Value</td>
<td>Other Value</td>
<td>Undefined</td>
</tr>
</tbody>
</table>

**rand()**

Returns a pseudorandom, uniformly distributed double between 0.0 and 1.0. Supported by SQL version 2015-10-8 and later.

Example:

`rand() = 0.8231909191640703`  

**regexp_matches(String, String)**

Returns whether the first argument contains a match for the second argument (regex).

Example:

`Regexp_matches("aaaa", "a\{2,\}") = true.`
Regexp_matches("aaaa", "b") = false.

**First argument:**

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>The String representation of the Int.</td>
</tr>
<tr>
<td>Decimal</td>
<td>The String representation of the Decimal.</td>
</tr>
<tr>
<td>Boolean</td>
<td>The String representation of the boolean (&quot;true&quot; or &quot;false&quot;).</td>
</tr>
<tr>
<td>String</td>
<td>The String.</td>
</tr>
<tr>
<td>Array</td>
<td>The String representation of the Array (using standard conversion rules).</td>
</tr>
<tr>
<td>Object</td>
<td>The String representation of the Object (using standard conversion rules).</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**Second argument:**

Must be a valid regex expression. Non-string types are converted to String using the standard conversion rules. Depending on the type, the resultant string may or may not be a valid regular expression. If the (converted) argument is not valid regex, the result is Undefined.

**Third argument:**

Must be a valid regex replacement string. (Can reference capture groups.) Non-string types will be converted to String using the standard conversion rules. If the (converted) argument is not a valid regex replacement string, the result is Undefined.

**regexp_replace(String, String, String)**

Replaces all occurrences of the second argument (regular expression) in the first argument with the third argument. Reference capture groups with "$". Supported by SQL version 2015-10-8 and later.

Example:

Regexp_replace("abcd", "bc", "x") = "axd".
Regexp_replace("abcd", "b(.*)d", "$1") = "ac".

**First argument:**

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>The String representation of the Int.</td>
</tr>
<tr>
<td>Decimal</td>
<td>The String representation of the Decimal.</td>
</tr>
<tr>
<td>Boolean</td>
<td>The String representation of the boolean (&quot;true&quot; or &quot;false&quot;).</td>
</tr>
<tr>
<td>String</td>
<td>The source value.</td>
</tr>
</tbody>
</table>
### Argument Type Result

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Array</td>
<td>The String representation of the Array (using standard conversion rules).</td>
</tr>
<tr>
<td>Object</td>
<td>The String representation of the Object (using standard conversion rules).</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**Second argument:**

Must be a valid regex expression. Non-string types are converted to Strings using the standard conversion rules. Depending on the type, the resultant string may or may not be a valid regular expression. If the (converted) argument is not a valid regex expression, the result is **Undefined**.

**Third argument:**

Must be a valid regex replacement string. (Can reference capture groups.) Non-string types will be converted to Strings using the standard conversion rules. If the (converted) argument is not a valid regex replacement string, the result is **Undefined**.

### regexp_substr(String, String)

Finds the first match of the 2nd parameter (regex) in the first parameter. Reference capture groups with "$". Supported by SQL version 2015-10-8 and later.

**Example:**

```sql
regexp_substr("hihihello", "hi") => "hi"
regexp_substr("hihihello", "(hi)*") => "hihi".
```

### First argument:

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>The String representation of the Int.</td>
</tr>
<tr>
<td>Decimal</td>
<td>The String representation of the Decimal.</td>
</tr>
<tr>
<td>Boolean</td>
<td>The String representation of the boolean (&quot;true&quot; or &quot;false&quot;).</td>
</tr>
<tr>
<td>String</td>
<td>The String argument.</td>
</tr>
<tr>
<td>Array</td>
<td>The String representation of the Array (using standard conversion rules).</td>
</tr>
<tr>
<td>Object</td>
<td>The String representation of the Object (using standard conversion rules).</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**Second argument:**
Must be a valid regex expression. Non-string types are converted to Strings using the standard conversion rules. Depending on the type, the resultant string may or may not be a valid regular expression. If the (converted) argument is not a valid regex expression, the result is Undefined.

Third argument:
Must be a valid regex replacement string. (Can reference capture groups.) Non-string types will be converted to String using the standard conversion rules. If the argument is not a valid regex replacement string, the result is Undefined.

**rpad(String, Int)**

Returns the string argument, padded on the right side with the number of spaces specified in the second argument. The Int argument must be between 0 and 1000. If the provided value is outside of this valid range, the argument will be set to the nearest valid value (0 or 1000). Supported by SQL version 2015-10-8 and later.

Examples:

```
rpad("hello", 2) = "hello ".
rpad(1, 3) = "1 ".
```

<table>
<thead>
<tr>
<th>argument Type 1</th>
<th>argument Type 2</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>Int</td>
<td></td>
</tr>
<tr>
<td>String</td>
<td>Decimal</td>
<td></td>
</tr>
<tr>
<td>argument Type 1</td>
<td>argument Type 2</td>
<td>Result</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>--------</td>
</tr>
<tr>
<td>String</td>
<td>String</td>
<td>The second argument will be converted to a Decimal, which is rounded down to the nearest Int. The String is padded on the right side with a number of spaces equal to the Int value.</td>
</tr>
</tbody>
</table>

with a number of spaces equal to the provided Int.
### round(Decimal)

Rounds the given Decimal to the nearest Int. If the Decimal is equidistant from two Int values (for example, 0.5), the Decimal is rounded up. Supported by SQL version 2015-10-8 and later.

**Example:**
- Round(1.2) = 1.
- Round(1.5) = 2.
- Round(1.7) = 2.
- Round(-1.1) = -1.
- Round(-1.5) = -2.

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>The argument.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Decimal is rounded down to the nearest Int.</td>
</tr>
<tr>
<td>String</td>
<td>String is rounded down to the nearest Int. If the string cannot be converted to a Decimal, the result is Undefined.</td>
</tr>
</tbody>
</table>
### Argument Type | Result
---|---
Other Value | Undefined.

**rtrim(String)**

Removes all trailing whitespace (tabs and spaces) from the provided String. Supported by SQL version 2015-10-8 and later.

Examples:

```
rtrim(" h i ") = " h i"
```

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>The String representation of the Int.</td>
</tr>
<tr>
<td>Decimal</td>
<td>The String representation of the Decimal.</td>
</tr>
<tr>
<td>Boolean</td>
<td>The String representation of the boolean (&quot;true&quot; or &quot;false&quot;).</td>
</tr>
<tr>
<td>Array</td>
<td>The String representation of the Array (using standard conversion rules).</td>
</tr>
<tr>
<td>Object</td>
<td>The String representation of the Object (using standard conversion rules).</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined</td>
</tr>
</tbody>
</table>

**sign(Decimal)**

Returns the sign of the given number. When the sign of the argument is positive, 1 is returned. When the sign of the argument is negative, -1 is returned. If the argument is 0, 0 is returned. Supported by SQL version 2015-10-8 and later.

Examples:

```
sign(-7) = -1.
sign(0) = 0.
sign(13) = 1.
```

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Int, the sign of the Int value.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Int, the sign of the Decimal value.</td>
</tr>
<tr>
<td>String</td>
<td>Int, the sign of the Decimal value. The string is converted to a Decimal value, and the sign of the Decimal value is returned. If the String cannot be converted to a Decimal, the result is Undefined. Supported by SQL version 2015-10-8 and later.</td>
</tr>
</tbody>
</table>
### sin(Decimal)

Returns the sine of a number in radians. Decimal arguments are rounded to double precision before function application. Supported by SQL version 2015-10-8 and later.

**Example:** sin(0) = 0.0

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Decimal (with double precision), the sine of the argument.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Decimal (with double precision), the sine of the argument.</td>
</tr>
<tr>
<td>Boolean</td>
<td>Undefined.</td>
</tr>
<tr>
<td>String</td>
<td>Decimal (with double precision), the sine of the argument. If the string cannot be converted to a Decimal, the result is Undefined.</td>
</tr>
<tr>
<td>Array</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

### sinh(Decimal)

Returns the hyperbolic sine of a number. Decimal values are rounded to double precision before function application. The result is a Decimal value of double precision. Supported by SQL version 2015-10-8 and later.

**Example:** sinh(2.3) = 4.936961805545957

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Decimal (with double precision), the hyperbolic sine of the argument.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Decimal (with double precision), the hyperbolic sine of the argument.</td>
</tr>
<tr>
<td>Boolean</td>
<td>Undefined.</td>
</tr>
<tr>
<td>String</td>
<td>Decimal (with double precision), the hyperbolic sine of the argument. If the string cannot be converted to a Decimal, the result is Undefined.</td>
</tr>
<tr>
<td>Array</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Argument Type</td>
<td>Result</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**substring(String, Int [, Int])**

Expects a `String` followed by one or two `Int` values. For a `String` and a single `Int` argument, this function returns the substring of the provided `String` from the provided `Int` index (0-based, inclusive) to the end of the `String`. For a `String` and two `Int` arguments, this function returns the substring of the provided `String` from the first `Int` index argument (0-based, inclusive) to the second `Int` index argument (0-based, exclusive). Indices that are less than zero will be set to zero. Indices that are greater than the `String` length will be set to the `String` length. For the three argument version, if the first index is greater than (or equal to) the second index, the result is the empty `String`.

If the arguments provided are not (`String`, `Int`), or (`String`, `Int`, `Int`), the standard conversions will be applied to the arguments to attempt to convert them into the correct types. If the types cannot be converted, the result of the function is `Undefined`. Supported by SQL version 2015-10-8 and later.

**Examples:**

```plaintext
substring("012345", 0) = "012345".
substring("012345", 2) = "2345".
substring("012345", 2.745) = "2345".
substring(123, 2) = "3".
substring("012345", -1) = "012345".
substring(true, 1.2) = "rue".
substring(false, -2.411E247) = "false".
substring("012345", 1, 3) = "12".
substring("012345", -50, 50) = "012345".
substring("012345", 3, 1) = "."
```

**sqrt(Decimal)**

Returns the square root of a number. `Decimal` arguments are rounded to double precision before function application. Supported by SQL version 2015-10-8 and later.

**Example:** `sqrt(9) = 3.0`
### Argument Type

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean</td>
<td>Undefined.</td>
</tr>
<tr>
<td>String</td>
<td>The square root of the argument. If the string cannot be converted to a Decimal, the result is Undefined.</td>
</tr>
<tr>
<td>Array</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

### startswith(String, String)

Returns Boolean, whether the first string argument starts with the second string argument. If either argument is Null or Undefined, the result is Undefined. Supported by SQL version 2015-10-8 and later.

Example:

```
startswith("ranger", "ran") = true
```

### tan(Decimal)

Returns the tangent of a number in radians. Decimal values are rounded to double precision before function application. Supported by SQL version 2015-10-8 and later.

Example: \( \tan(3) = -0.1425465430742778 \)
<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

### tanh(Decimal)

Returns the hyperbolic tangent of a number in radians. `Decimal` values are rounded to double precision before function application. Supported by SQL version 2015-10-8 and later.

Example: \( \text{tanh}(2.3) = 0.9800963962661914 \)

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Decimal (with double precision), the hyperbolic tangent of the argument.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Decimal (with double precision), the hyperbolic tangent of the argument.</td>
</tr>
<tr>
<td>Boolean</td>
<td>Undefined.</td>
</tr>
<tr>
<td>String</td>
<td>Decimal (with double precision), the hyperbolic tangent of the argument. If the string cannot be converted to a <code>Decimal</code>, the result is <code>Undefined</code>.</td>
</tr>
<tr>
<td>Array</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Object</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

### timestamp()

Returns the current timestamp in milliseconds from 00:00:00 Coordinated Universal Time (UTC), Thursday, 1 January 1970, as observed by the AWS IoT rules engine. Supported by SQL version 2015-10-8 and later.

Example: \( \text{timestamp()} = 1481825251155 \)

### topic(Decimal)

Returns the topic to which the message that triggered the rule was sent. If no parameter is specified, the entire topic is returned. The `Decimal` parameter is used to specify a specific, one-based topic segment. For the topic `foo/bar/baz`, `topic(1)` will return `foo`, `topic(2)` will return `bar`, and so on. Supported by SQL version 2015-10-8 and later.

Examples:

\( \text{topic()} = \text{"things/myThings/thingOne"} \)

\( \text{topic(1)} = \text{"things"} \)
traceid()

Returns the trace ID (UUID) of the MQTT message, or Undefined if the message wasn't sent over MQTT. Supported by SQL version 2015-10-8 and later.

Example:

```
traceid() = "12345678-1234-1234-1234-123456789012"
```

trunc(Decimal, Int)

Truncates the first argument to the number of Decimal places specified by the second argument. If the second argument is less than zero, it will be set to zero. If the second argument is greater than 34, it will be set to 34. Trailing zeroes are stripped from the result. Supported by SQL version 2015-10-8 and later.

Examples:

```
trunc(2.3, 0) = 2.
trunc(2.3123, 2) = 2.31.
trunc(2.888, 2) = 2.88.
(2.00, 5) = 2.
```

<table>
<thead>
<tr>
<th>argument Type 1</th>
<th>argument Type 2</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>Int</td>
<td>The source value.</td>
</tr>
<tr>
<td>Int/Decimal</td>
<td>Int/Decimal</td>
<td>The first argument is truncated to the length described by the second argument. The second argument, if not an Int, will be rounded down to the nearest Int. Strings are converted to Decimal values. If the string conversion fails, the result is Undefined.</td>
</tr>
<tr>
<td>Int/Decimal/String</td>
<td>The first argument is truncated to the length described by the second argument. The second argument, if not an Int, will be rounded down to the nearest Int. Strings are converted to Decimal values. If the string conversion fails, the result is Undefined.</td>
<td></td>
</tr>
<tr>
<td>Other Value</td>
<td>Undefined</td>
<td></td>
</tr>
</tbody>
</table>

trim(String)

Removes all leading and trailing whitespace from the provided String. Supported by SQL version 2015-10-8 and later.

Example:

```
Trim(" hi ") = "hi"
```

<table>
<thead>
<tr>
<th>Argument Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int</td>
<td>The String representation of the Int with all leading and trailing whitespace removed.</td>
</tr>
<tr>
<td>Decimal</td>
<td>The String representation of the Decimal with all leading and trailing whitespace removed.</td>
</tr>
<tr>
<td>Argument Type</td>
<td>Result</td>
</tr>
<tr>
<td>---------------</td>
<td>--------</td>
</tr>
<tr>
<td>Boolean</td>
<td>The String representation of the Boolean (&quot;true&quot; or &quot;false&quot;) with all leading and trailing whitespace removed.</td>
</tr>
<tr>
<td>String</td>
<td>The String with all leading and trailing whitespace removed.</td>
</tr>
<tr>
<td>Array</td>
<td>The String representation of the Array using standard conversion rules.</td>
</tr>
<tr>
<td>Object</td>
<td>The String representation of the Object using standard conversion rules.</td>
</tr>
<tr>
<td>Null</td>
<td>Undefined.</td>
</tr>
<tr>
<td>Undefined</td>
<td>Undefined.</td>
</tr>
</tbody>
</table>

**upper(String)**

Returns the uppercase version of the given String. Non-String arguments are converted to String using the standard conversion rules. Supported by SQL version 2015-10-8 and later.

Examples:

`upper("hello") = "HELLO"`

`upper(["hello"]) = ["HELLO"]`

**SELECT Clause**

The AWS IoT SELECT clause is essentially the same as the ANSI SQL SELECT clause, with some minor differences.

You can use the SELECT clause to extract information from incoming MQTT messages. **SELECT ** can be used to retrieve the entire incoming message payload. For example:

```
Incoming payload published on topic 'a/b': {"color":"red", "temperature":50}
SQL statement: SELECT * FROM 'a/b'
Outgoing payload: {"color":"red", "temperature":50}
```

If the payload is a JSON object, you can reference keys in the object. Your outgoing payload will contain the key-value pair. For example:

```
Incoming payload published on topic 'a/b': {"color":"red", "temperature":50}
SQL statement: SELECT color FROM 'a/b'
Outgoing payload: {"color":"red"}
```

You can use the **AS** keyword to rename keys. For example:

```
Incoming payload published on topic 'a/b': {"color":"red", "temperature":50}
SQL:SELECT color AS my_color FROM 'a/b'
Outgoing payload: {"my_color":"red"}
```

You can select multiple items by separating them with a comma. For example:
Incoming payload published on topic 'a/b': {"color":"red", "temperature":50}
SQL: SELECT color as my_color, temperature as farenheit FROM 'a/b'
Outgoing payload: {"my_color":"red","farenheit":50}

You can select multiple items including '*' to add items to the incoming payload. For example:

Incoming payload published on topic 'a/b': {"color":"red", "temperature":50}
SQL: SELECT *, 15 as speed FROM 'a/b'
Outgoing payload: {"color":"red", "temperature":50, speed:15}"

You can use the "VALUE" keyword to produce outgoing payloads that are not JSON objects. You may only select one item. For example:

Incoming payload published on topic 'a/b': {"color":"red", "temperature":50}
SQL: SELECT VALUE color FROM 'a/b'
Outgoing payload: "red"

You can use "." syntax to drill into nested JSON objects in the incoming payload. For example:

Incoming payload published on topic 'a/b': {"color":{"red":255,"green":0,"blue":0},
"temperature":50}  
SQL: SELECT color.red as red_value FROM 'a/b'
Outgoing payload: {"red_value":255}

You can use functions (see Functions (p. 209)) to transform the incoming payload. Parentheses can be used for grouping. For example:

Incoming payload published on topic 'a/b': {"color":"red", "temperature":50}
SQL: SELECT (temperature – 32) * 5 / 9 AS celsius, upper(color) as my_color FROM 'a/b'
Outgoing payload: {"celsius":10,"my_color":"RED"}

Working with Binary Payloads

When the message payload should be handled as raw binary data (rather than a JSON object), you can use the * operator to refer to it in a SELECT clause.

These rules must be followed to use * to refer to the message payload as raw binary data:

1. The SQL statement and templates must not refer to JSON names, other than *.
2. The SELECT statement must have * as the only item, or must have only functions, for example:

   SELECT * FROM 'a/b'

   SELECT encode(*, 'base64') AS data, timestamp() AS ts FROM 'a/b'

Binary Payload Examples

The following SELECT clause can be used with binary payloads because it doesn't refer to any JSON names.

SELECT * FROM 'a/b'
The following SELECT cannot be used with binary payloads because it refers to device_type in the WHERE clause.

```
SELECT * FROM 'a/b' WHERE device_type = 'thermostat'
```

The following SELECT cannot be used with binary payloads because it violates rule #2.

```
SELECT *, timestamp() AS timestamp FROM 'a/b'
```

The following SELECT can be used with binary payloads because it doesn’t violate either rule #1 or #2.

```
SELECT * FROM 'a/b' WHERE timestamp() % 12 = 0
```

The following AWS IoT rule cannot be used with payloads because it violates rule #1.

```
{
  "sql": "SELECT * FROM 'a/b''
  "actions": [{
    "republish": {
      "topic": "device/${device_id}"
    }
  }]
}
```

FROM Clause

The FROM clause subscribes your rule to a topic or topic filter. A topic filter allows you to subscribe to a group of similar topics.

Example:

Incoming payload published on topic 'a/b': {temperature: 50}

Incoming payload published on topic 'a/c': {temperature: 50}

SQL: "SELECT temperature AS t FROM 'a/b'."

The rule is subscribed to 'a/b', so the incoming payload is passed to the rule, and the outgoing payload (passed to the rule actions) is: {t: 50}. The rule is not subscribed to 'a/c', so the rule is not triggered for the message published on 'a/c'.

You can use the # wildcard character to match any subpath in a topic filter:

Example:

Incoming payload published on topic 'a/b': {temperature: 50}.

Incoming payload published on topic 'a/c': {temperature: 60}.

Incoming payload published on topic 'a/e/f': {temperature: 70}.

Incoming payload published on topic 'b/x': {temperature: 80}.

SQL: "SELECT temperature AS t FROM 'a/#'."

The rule is subscribed to any topic beginning with 'a', so it is executed three times, sending outgoing payloads of {t: 50} (for a/b), {t: 60} (for a/c), and {t: 70} (for a/e/f) to its actions. It is not subscribed to 'b/x', so the rule will not be triggered for the {temperature: 80} message.
WHERE Clause

The WHERE clause determines if a rule is evaluated for a message sent to an MQTT topic to which the rule is subscribed. If the WHERE clause evaluates to true, the rule is evaluated. Otherwise, the rule is not evaluated.

Example:

Incoming payload published on topic 'a/b': {temperature: 50}.
Incoming payload published on topic 'a/c': {temperature: 60}.
Incoming payload published on topic 'a/e/f': {temperature: 70}.
Incoming payload published on topic 'b/x': {temperature: 80}.

SQL: "SELECT temperature AS t FROM 'a/+'".

The rule is subscribed to all topics with two path elements where the first element is 'a'. The rule is executed for the messages sent to 'a/b' and 'a/c', but not 'a/e/f' or 'b/x'.

You can use functions and operators in the WHERE clause. In the WHERE clause, you cannot reference any aliases created with the AS keyword in the SELECT. (The WHERE clause is evaluated first, to determine if the SELECT clause is evaluated.)

Literals

You can directly specify literal objects in the SELECT and WHERE clauses of your rule SQL, which can be useful for passing information.

Note

Literals are only available when using SQL Version 2016-03-23 or newer.

JSON object syntax is used (key-value pairs, comma-separated, where keys are strings and values are JSON values, wrapped in curly brackets {}). For example:

Incoming payload published on topic a/b: {"lat_long": [47.606,-122.332]}

SQL statement: SELECT {'latitude': get(lat_long, 0), 'longitude':get(lat_long, 1)} as lat_long FROM 'a/b'

The resulting outgoing payload would be: {"latitude":47.606,"longitude":-122.332}.
You can also directly specify arrays in the SELECT and WHERE clauses of your rule SQL, which allows you to group information. JSON syntax is used (wrap comma-separated items in square brackets [] to create an array literal). For example:

Incoming payload published on topic a/b: {"lat": 47.696, "long": -122.332}

SQL statement: SELECT [lat,long] as lat_long FROM 'a/b'

The resulting output payload would be: {"lat_long": [47.606,-122.332]}.

Case Statements

Case statements can be used for branching execution, like a switch statement, or if/else statements.

Syntax:

```
CASE v WHEN t[1] THEN r[1]
    ... 
    WHEN t[n] THEN r[n]
    ELSE r[e] END
```

The expression v is evaluated and matched for equality against each t[i] expression. If a match is found, the corresponding r[i] expression becomes the result of the case statement. If there is more than one possible match, the first match is selected. If there are no matches, the else statement's re is used as the result. If there is no match and no else statement, the result of the case statement is Undefined. For example:

Incoming payload published on topic a/b: {"color":"yellow"}

SQL statement: SELECT CASE color WHEN 'green' THEN 'go' WHEN 'yellow' THEN 'caution' WHEN 'red' THEN 'stop' ELSE 'you are not at a stop light' END as instructions FROM 'a/b'

The resulting output payload would be: {"instructions":"caution"}.

Case statements require at least one WHEN clause. An ELSE clause is not required.

Note
If v is Undefined, the result of the case statement is Undefined.

JSON Extensions

You can use the following extensions to ANSI SQL syntax to make it easier to work with nested JSON objects.

"." Operator

This operator accesses members in embedded JSON objects and functions identically to ANSI SQL and JavaScript. For example:

```
SELECT foo.bar AS bar.baz FROM 'a/b'
```

* Operator

This functions in the same way as the * wildcard in ANSI SQL. It's used in the SELECT clause only and creates a new JSON object containing the message data. If the message payload is not in JSON format, * returns the entire message payload as raw bytes. For example:
Applying a Function to an Attribute Value

The following is an example JSON payload that could be published by a device:

```json
{
  "deviceid" : "iot123",
  "temp" : 54.98,
  "humidity" : 32.43,
  "coords" : {
    "latitude" : 47.615694,
    "longitude" : -122.3359976
  }
}
```

The following example applies a function to an attribute value in a JSON payload:

```sql
SELECT temp, md5(deviceid) AS hashed_id FROM topic/#
```

The result of this query is the following JSON object:

```json
{
  "temp": 54.98,
  "hashed_id": "e37f81fb397e595c4aeb5645b8cbbbd1"
}
```

Substitution Templates

You can use a substitution template to augment the JSON data returned when a rule is triggered and AWS IoT performs an action. The syntax for a substitution template is `$\{expression\}$`, where `expression` can be any expression supported by AWS IoT in SELECT or WHERE clauses. For more information about supported expressions, see AWS IoT SQL Reference (p. 200).

Substitution templates appear in the SELECT clause within a rule:

```json
{
  "sql": "SELECT *, topic() AS topic FROM 'my/iot/topic'",
  "ruleDisabled": false,
  "actions": [{
    "republish": {
      "topic": "#${topic()}/republish",
      "roleArn": "arn:aws:iam::123456789012:role/my-iot-role"
    }
  }]
}
```

If this rule is triggered by the following JSON:

```json
{
  "deviceid" : "iot123",
  "temp" : 54.98,
  "humidity" : 32.43,
  "coords" : {
    "latitude" : 47.615694,
    "longitude" : -122.3359976
  }
}
```
Here is the output of the rule:

```json
{
    "coords":{
        "longitude":-122.3359976,
        "latitude":47.615694
    },
    "humidity":32.43,
    "temp":54.98,
    "deviceid":"iot123",
    "topic":"my/iot/topic"
}
```
Device Shadow Service for AWS IoT

A device’s shadow is a JSON document that is used to store and retrieve current state information for a device. The Device Shadow service maintains a shadow for each device you connect to AWS IoT. You can use the shadow to get and set the state of a device over MQTT or HTTP, regardless of whether the device is connected to the Internet. Each device’s shadow is uniquely identified by the name of the corresponding thing.

Contents

- Device Shadow Service Data Flow (p. 249)
- Device Shadow Service Documents (p. 256)
- Using Shadows (p. 259)
- Device Shadow RESTful API (p. 268)
- Shadow MQTT Topics (p. 271)
- Shadow Document Syntax (p. 277)
- Shadow Error Messages (p. 279)

Device Shadow Service Data Flow

The Device Shadow service acts as an intermediary, allowing devices and applications to retrieve and update a device’s shadow.

To illustrate how devices and applications communicate with the Device Shadow service, this section walks you through the use of the AWS IoT MQTT client and the AWS CLI to simulate communication between an internet-connected light bulb, an application, and the Device Shadow service.

The Device Shadow service uses MQTT topics to facilitate communication between applications and devices. To see how this works, use the AWS IoT MQTT client to subscribe to the following MQTT topics with QoS 1:

$aws/things/myLightBulb/shadow/update/accepted

The Device Shadow service sends messages to this topic when an update is successfully made to the device’s shadow.

$aws/things/myLightBulb/shadow/update/rejected

The Device Shadow service sends messages to this topic when an update to the device’s shadow is rejected.

$aws/things/myLightBulb/shadow/update/delta

The Device Shadow service sends messages to this topic when a difference is detected between the reported and desired sections of the device’s shadow. For more information, see /update/delta (p. 273).

$aws/things/myLightBulb/shadow/get/accepted

The Device Shadow service sends messages to this topic when a request for the device’s shadow is made successfully.

$aws/things/myLightBulb/shadow/get/rejected

The Device Shadow service sends messages to this topic when a request for the device’s shadow is rejected.
$aws/things/myLightBulb/shadow/delete/accepted

The Device Shadow service sends messages to this topic when the device's shadow is deleted.

$aws/things/myLightBulb/shadow/delete/rejected

The Device Shadow service sends messages to this topic when a request to delete the device's shadow is rejected.

$aws/things/myLightBulb/shadow/update/documents

The Device Shadow service publishes a state document to this topic whenever an update to the device's shadow is successfully performed.

To learn more about all of the MQTT topics used by the Device Shadow service, see [Shadow MQTT Topics](#).  

**Note**

We recommend that you subscribe to the .../rejected topics to see any errors sent by the Device Shadow service.

When the light bulb comes online, it sends its current state to the Device Shadow service by sending an MQTT message to the $aws/things/myLightBulb/shadow/update topic.

To simulate this, use the AWS IoT MQTT client to publish the following message to the $aws/things/myLightbulb/shadow/update topic:

```
{
    "state": {
        "reported": {
            "color": "red"
        }
    }
}
```

This message sets the color of the light bulb to "red."

The Device Shadow service responds by sending the following message to the $aws/things/myLightBulb/shadow/update/accepted topic:

```
{
    "messageNumber": 4,
    "payload": {
        "state": {
            "reported": {
                "color": "red"
            }
        },
        "metadata": {
            "reported": {
                "color": {
                    "timestamp": 1469564492
                }
            }
        },
        "version": 1,
        "timestamp": 1469564492
    },
    "qos": 0,
    "timestamp": 1469564492848,
    "topic": "$aws/things/myLightBulb/shadow/update/accepted"
}
```
This message indicates the Device Shadow service received the UPDATE request and updated the device's shadow. If the shadow doesn't exist, it is created. Otherwise, the shadow is updated with the data in the message. If you don't see a message published to $aws/things/myLightBulb/shadow/update/accepted, check the subscription to $aws/things/myLightBulb/shadow/update/rejected to see any error messages.

In addition, the Device Shadow service publishes the following message to the $aws/things/myLightBulb/shadow/update/documents topic:

```json
{
    "previous":null,
    "current":{
        "state":{
            "reported":{
                "color":"red"
            }
        },
        "metadata":{
            "reported":{
                "color":{
                    "timestamp":1483467764
                }
            }
        },
        "version":1
    },
    "timestamp":1483467764
}
```

Messages are published to the /update/documents topic whenever an update to the device's shadow is successfully performed. For more information of the contents of messages published to this topic, see Shadow MQTT Topics (p. 271).

An application that interacts with the light bulb comes online and requests the light bulb's current state. The application sends an empty message to the $aws/things/myLightBulb/shadow/get topic. To simulate this, use the AWS IoT MQTT client to publish an empty message (""") to the $aws/things/myLightBulb/shadow/get topic.

The Device Shadow service responds by publishing the requested shadow to the $aws/things/myLightBulb/shadow/get/accepted topic:

```json
{
    "messageNumber": 1,
    "payload": {
        "state": {
            "reported": {
                "color": "red"
            }
        },
        "metadata": {
            "reported": {
                "color": {
                    "timestamp": 1469564492
                }
            }
        },
        "version": 1,
        "timestamp": 1469564571
    },
    "qos": 0,
    "timestamp": 1469564571533,
    "topic": "$aws/things/myLightBulb/shadow/get/accepted"
}
```
If you don’t see a message on the $aws/things/myLightBulb/shadow/get/accepted topic, check the $aws/things/myLightBulb/shadow/get/rejected topic for any error messages.

The application displays this information to the user, and the user requests a change to the light bulb’s color (from red to green). To do this, the application publishes a message on the $aws/things/myLightBulb/shadow/update topic:

```
{
    "state": {
        "desired": {
            "color": "green"
        }
    },
    "metadata": {
        "desired": {
            "color": {
                "timestamp": 1469564658
            }
        }
    },
    "version": 2,
    "timestamp": 1469564658
}
```

To simulate this, use the AWS IoT MQTT client to publish the preceding message to the $aws/things/myLightBulb/shadow/update topic.

The Device Shadow service responds by sending a message to the $aws/things/myLightBulb/shadow/update/accepted topic:

```
{
    "messageNumber": 5,
    "payload": {
        "state": {
            "desired": {
                "color": "green"
            }
        },
        "metadata": {
            "desired": {
                "color": {
                    "timestamp": 1469564658
                }
            }
        },
        "version": 2,
        "timestamp": 1469564658
    },
    "qos": 0,
    "timestamp": 1469564658286,
    "topic": "$aws/things/myLightBulb/shadow/update/accepted"
}
```

and to the $aws/things/myLightBulb/shadow/update/delta topic:

```
{
    "messageNumber": 1,
    "payload": {
        "version": 2,
        "timestamp": 1469564658,
        "state": {
            "color": "green"
        },
        "metadata": {
            "color": {
                "timestamp": 1469564658
            }
        }
    }
}
```
The Device Shadow service publishes a message to this topic when it accepts a shadow update and the resulting shadow contains different values for desired and reported states.

The Device Shadow service also publishes a message to the $aws/things/myLightBulb/shadow/update/documents topic:

```
{
  "previous": {
    "state": {
      "reported": {
        "color": "red"
      }
    },
    "metadata": {
      "reported": {
        "color": {
          "timestamp": 1483467764
        }
      }
    },
    "version": 1
  },
  "current": {
    "state": {
      "desired": {
        "color": "green"
      },
      "reported": {
        "color": "red"
      }
    },
    "metadata": {
      "desired": {
        "color": {
          "timestamp": 1483468612
        }
      },
      "reported": {
        "color": {
          "timestamp": 1483467764
        }
      }
    },
    "version": 2
  },
  "timestamp": 1483468612
}
```

The light bulb is subscribed to the $aws/things/myLightBulb/shadow/update/delta topic, so it receives the message, changes its color, and publishes its new state. To simulate this, use the AWS IoT MQTT client to publish the following message to the $aws/things/myLightBulb/shadow/update topic to update the shadow state:

```
{
  "state": {
    "reported": {
      "color": "green"
    }
  },
  "timestamp": 1483468612
}
```
In response, the Device Shadow service sends a message to the $aws/things/myLightBulb/shadow/update/accepted topic:

```
{
   "messageNumber": 6,
   "payload": {
      "state": {
         "reported": {
            "color": "green"
         },
         "desired": null
      },
      "metadata": {
         "reported": {
            "color": {
               "timestamp": 1469564801
            }
         },
         "desired": {
            "timestamp": 1469564801
         }
      },
      "version": 3,
      "timestamp": 1469564801
   },
   "qos": 0,
   "timestamp": 1469564801673,
   "topic": "$aws/things/myLightBulb/shadow/update/accepted"
}
```

and to the $aws/things/myLightBulb/shadow/update/documents topic:

```
{
   "previous":{
      "state":{
         "reported":{
            "color": "red"
         }
      },
      "metadata":{
         "reported":{
            "color":{
               "timestamp":1483470355
            }
         }
      },
      "version":3
   },
   "current":{
      "state":{
         "reported":{
            "color": "green"
         }
      },
      "metadata":{
         "reported":{
            "color":{
               "timestamp":1483470364
            }
         }
      }
   }
}
```
The app requests the current state from the Device Shadow service and displays the most recent state data. To simulate this, run the following command:

```
aws iot-data get-thing-shadow --thing-name "myLightBulb" "output.txt" && cat "output.txt"
```

**Note**

On Windows, omit the `&& cat "output.txt"`, which displays the contents of output.txt to the console. You can open the file in Notepad or any text editor to see the contents of the shadow.

The Device Shadow service returns the shadow document:

```
{
    "state": {
        "reported": {
            "color": "green"
        }
    },
    "metadata": {
        "reported": {
            "color": {
                "timestamp": 1469564801
            }
        }
    },
    "version": 3,
    "timestamp": 1469564864
}
```

To delete the device's shadow, publish an empty message to the `$aws/things/myLightBulb/shadow/delete` topic. AWS IoT responds by publishing a message to the `$aws/things/myLightBulb/shadow/delete/accepted` topic:

```
{
    "version": 1,
    "timestamp": 1488565234
}
```

**Detecting a Thing Is Connected**

To determine if a device is currently connected, include a connected setting in the shadow and use an MQTT Last Will and Testament (LWT) message that sets the connected setting to `false` if a device is disconnected due to error.

**Note**

Currently, LWT messages sent to AWS IoT reserved topics (topics that begin with `$`) are ignored by the AWS IoT Device Shadow service, but are still processed by subscribed clients and by the AWS IoT rules engine. If you want the Device Shadow service to receive LWT messages, register an LWT message to a non-reserved topic and create a rule that republishes the message on the reserved topic. The following example shows how to create a republish rule that listens for a messages from the `my/things/myLightBulb/update` topic and republishes it to `$aws/things/myLightBulb/shadow/update`.
When a device connects, it registers an LWT that sets the connected setting to false:

```json
{
    "state": {
        "reported": {
            "connected": "false"
        }
    }
}
```

It also publishes a message on its update topic ($aws/things/myLightBulb/shadow/update), setting its connected state to true:

```json
{
    "state": {
        "reported": {
            "connected": "true"
        }
    }
}
```

When the device disconnects gracefully, it publishes a message on its update topic and sets its connected state to false:

```json
{
    "state": {
        "reported": {
            "connected": "false"
        }
    }
}
```

If the device disconnects due to an error, its LWT message is posted automatically to the update topic.

# Device Shadow Service Documents

The Device Shadow service respects all rules of the JSON specification. Values, objects, and arrays are stored in the device's shadow document.

## Contents
- Document Properties (p. 257)
Document Properties

A device's shadow document has the following properties:

- **state**
  - **desired**
    - The desired state of the thing. Applications can write to this portion of the document to update the state of a thing without having to directly connect to a thing.
  - **reported**
    - The reported state of the thing. Things write to this portion of the document to report their new state. Applications read this portion of the document to determine the state of a thing.

- **metadata**
  - Information about the data stored in the state section of the document. This includes timestamps, in Epoch time, for each attribute in the state section, which enables you to determine when they were updated.

- **timestamp**
  - Indicates when the message was transmitted by AWS IoT. By using the timestamp in the message and the timestamps for individual attributes in the desired or reported section, a thing can determine how old an updated item is, even if it doesn't feature an internal clock.

- **clientToken**
  - A string unique to the device that enables you to associate responses with requests in an MQTT environment.

- **version**
  - The document version. Every time the document is updated, this version number is incremented. Used to ensure the version of the document being updated is the most recent.

For more information, see Shadow Document Syntax (p. 277).

Versioning of a Device Shadow

The Device Shadow service supports versioning on every update message (both request and response), which means that with every update of a device's shadow, the version of the JSON document is incremented. This ensures two things:

- A client can receive an error if it attempts to overwrite a shadow using an older version number. The client is informed it must resync before it can update a device's shadow.
- A client can decide not to act on a received message if the message has a lower version than the version stored by the client.

In some cases, a client might bypass version matching by not submitting a version.
Client Token

You can use a client token with MQTT-based messaging to verify the same client token is contained in a request and request response. This ensures the response and request are associated.

**Note**
The client token can be no longer than 64 bytes. A client token that is longer than 64 bytes will cause a 400 (Bad Request) response and an *Invalid clientToken* error message.

Example Document

Here is an example shadow document:

```json
{
  "state" : {
    "desired" : {
      "color" : "RED",
      "sequence" : [ "RED", "GREEN", "BLUE" ]
    },
    "reported" : {
      "color" : "GREEN"
    }
  },
  "metadata" : {
    "desired" : {
      "color" : {
        "timestamp" : 12345
      },
      "sequence" : {
        "timestamp" : 12345
      }
    },
    "reported" : {
      "color" : {
        "timestamp" : 12345
      }
    }
  },
  "version" : 10,
  "clientToken" : "UniqueClientToken",
  "timestamp": 123456789
}
```

Empty Sections

A shadow document contains a *desired* section only if it has a desired state. For example, the following is a valid state document with no *desired* section:

```json
{
  "reported" : { "temp": 55 }
}
```

The *reported* section can also be empty:

```json
{
  "desired" : { "color" : "RED" }
}
```
If an update causes the desired or reported sections to become null, the section is removed from the document. To remove the desired section from a document (in response, for example, to a device updating its state), set the desired section to null:

```
{
    "state": {
        "reported": {
            "color": "red"
        },
        "desired": null
    }
}
```

It is also possible a shadow document will not contain desired or reported sections. In that case, the shadow document is empty. For example, this is a valid document:

```
{
}
```

## Arrays

Shadows support arrays, but treat them as normal values in that an update to an array replaces the whole array. It is not possible to update part of an array.

**Initial state:**

```
{
    "desired": { "colors": ["RED", "GREEN", "BLUE"] }
}
```

**Update:**

```
{
    "desired": { "colors": ["RED"] }
}
```

**Final state:**

```
{
    "desired": { "colors": ["RED"] }
}
```

Arrays can't have null values. For example, the following array is not valid and will be rejected.

```
{
    "desired": {
        "colors": [ null, "RED", "GREEN"]
    }
}
```

## Using Shadows

AWS IoT provides three methods for working with a device's shadow:
UPDATE

Creates a device's shadow if it doesn't exist, or updates the contents of a device's shadow with the data provided in the request. The data is stored with timestamp information to indicate when it was last updated. Messages are sent to all subscribers with the difference between desired or reported state (delta). Things or apps that receive a message can perform an action based on the difference between desired or reported states. For example, a device can update its state to the desired state, or an app can update its UI to show the change in the device's state.

GET

Retrieves the latest state stored in the device's shadow (for example, during start-up of a device to retrieve configuration and the last state of operation). This method returns the full JSON document, including metadata.

DELETE

Deletes a device's shadow, including all of its content. This removes the JSON document from the data store. You can't restore a device's shadow you deleted, but you can create a new shadow with the same name.

Protocol Support

These methods are supported through both MQTT and a RESTful API over HTTPS. Because MQTT is a publish/subscribe communication model, AWS IoT implements a set of reserved topics. Things or applications subscribe to these topics before publishing on a request topic in order to implement a request–response behavior. For more information, see Shadow MQTT Topics (p. 271) and Device Shadow RESTful API (p. 268).

Updating a Shadow

You can update a device's shadow by using the UpdateThingShadow (p. 269) RESTful API or by publishing to the /update (p. 271) topic. Updates affect only the fields specified in the request.

Initial state:

```json
{
    "state": {
        "reported": {
            "color": { "r": 255, "g": 255, "b": 0 }
        }
    }
}
```

An update message is sent:

```json
{
    "state": {
        "desired": {
            "color": { "r": 10 },
            "engine": "ON"
        }
    }
}
```

The device receives the desired state on the /update/delta topic that is triggered by the previous /update message and then executes the desired changes. When finished, the device should confirm its updated state through the reported section in the shadow JSON document.
Final state:

```json
{
  "state": {
    "reported": {
      "color": { "r": 10, "g": 255, "b": 0 },
      "engine": "ON"
    }
  }
}
```

## Retrieving a Shadow Document

You can retrieve a device's shadow by using the `GetThingShadow` (p. 269) RESTful API or by subscribing and publishing to the `/get` (p. 274) topic. This retrieves the entire document plus the delta between the desired or reported states.

**Example document:**

```json
{
  "state": {
    "desired": {
      "lights": {
        "color": "RED"
      },
      "engine": "ON"
    },
    "reported": {
      "lights": {
        "color": "GREEN"
      },
      "engine": "ON"
    },
    "metadata": {
      "desired": {
        "lights": {
          "color": {
            "timestamp": 123456
          },
          "engine": {
            "timestamp": 123456
          }
        }
      },
      "reported": {
        "lights": {
          "color": {
            "timestamp": 789012
          },
          "engine": {
            "timestamp": 789012
          }
        }
      },
      "version": 10,
      "timestamp": 123456789
    }
  }
}
```

**Response:**

261
Optimistic Locking

You can use the state document version to ensure you are updating the most recent version of a device's shadow document. When you supply a version with an update request, the service rejects the request with an HTTP 409 conflict response code if the current version of the state document does not match the version supplied.

For example:

Initial document:
Deleting Data

You can delete data from a device's shadow by publishing to the `/update (p. 271)` topic, setting the fields to be deleted to null. Any field with a value of `null` is removed from the document.

Initial state:

```json
{

}
```
Deleting a Shadow

An update message is sent:

```
{
  "state": {
    "desired": null,
    "reported": {
      "engine": null
    }
  }
}
```

Final state:

```
{
  "state": {
    "reported": {
      "lights": { "color" : "GREEN" }
    }
  }
}
```

You can delete all data from a device's shadow by setting its state to null. For example, sending the following message deletes all of the state data, but the device's shadow remains:

```
{
  "state": null
}
```

The device's shadow still exists even if its state is null. The version of the shadow is incremented when the next update occurs.

Deleting a Shadow

You can delete a device's shadow document by using the `DeleteThingShadow (p. 270)` RESTful API or by publishing to the `/delete (p. 275)` topic.

**Note**
Deleting a device's shadow does not delete the thing. Deleting a thing does not delete the corresponding device's shadow.

Initial state:

```
{
  "state": {
    "desired": {
      "lights": { "color": "RED" },
      "engine": "ON"
    },
    "reported": {
      "lights": { "color": "GREEN" },
      "engine": "OFF"
    }
  }
}
```
Delta State

Delta state is a virtual type of state that contains the difference between the desired and reported states. Fields in the desired section that are not in the reported section are included in the delta. Fields that are in the reported section and not in the desired section are not included in the delta. The delta contains metadata, and its values are equal to the metadata in the desired field. For example:

```json
{
    "state": {
        "desired": {
            "color": "RED",
            "state": "STOP"
        },
        "reported": {
            "color": "GREEN",
            "engine": "ON"
        },
        "delta": {
            "color": "RED",
            "state": "STOP"
        }
    },
    "metadata": {
        "desired": {
            "color": {
                "timestamp": 12345
            },
            "state": {
                "timestamp": 12345
            }
        },
        "reported": {
            "color": {
                "timestamp": 12345
            },
            "engine": {
                "timestamp": 12345
            }
        },
        "delta": {
            "color": {
                "timestamp": 12345
            },
            "state": {
                "timestamp": 12345
            }
        }
    }
}
```
When nested objects differ, the delta contains the path all the way to the root.

```json
{
    "state": {
        "desired": {
            "lights": {
                "color": {
                    "r": 255,
                    "g": 255,
                    "b": 255
                }
            }
        },
        "reported": {
            "lights": {
                "color": {
                    "r": 255,
                    "g": 0,
                    "b": 255
                }
            }
        },
        "delta": {
            "lights": {
                "color": {
                    "g": 255
                }
            }
        }
    },
    "version": 18,
    "timestamp": 123456789
}
```

The Device Shadow service calculates the delta by iterating through each field in the desired state and comparing it to the reported state.

Arrays are treated like values. If an array in the desired section doesn't match the array in the reported section, then the entire desired array is copied into the delta.

### Observing State Changes

When a device's shadow is updated, messages are published on two MQTT topics:

- `$aws/things/thing-name/shadow/update/accepted`
- `$aws/things/thing-name/shadow/update/delta`

The message sent to the update/delta topic is intended for the thing whose state is being updated. This message contains only the difference between the desired and reported sections of the device's shadow document. Upon receiving this message, the device should decide whether to make the requested change. If the device's state is changed, it should publish its new current state to the `$aws/things/thing-name/shadow/update` topic.

Devices and applications can subscribe to either of these topics to be notified when the state of the document has changed.
Here is an example of that flow:

1. A device reports its state.
2. The system updates the state document in its persistent data store.
3. The system publishes a delta message, which contains only the delta and is targeted at the subscribed devices. Devices should subscribe to this topic to receive updates.
4. The device's shadow publishes an accepted message, which contains the entire received document, including metadata. Applications should subscribe to this topic to receive updates.

**Message Order**

There is no guarantee that messages from the AWS IoT service will arrive at the device in any specific order.

Initial state document:

```json
{
    "state": {
        "reported": { "color" : "blue" }
    },
    "version" : 10,
    "timestamp": 123456777
}
```

Update 1:

```json
{
    "state": { "desired" : { "color" : "RED" } },
    "version": 10,
    "timestamp": 123456777
}
```

Update 2:

```json
{
    "state": { "desired" : { "color" : "GREEN" } },
    "version": 11,
    "timestamp": 123456778
}
```

Final state document:

```json
{
    "state": {
        "reported": { "color" : "GREEN" }
    },
    "version": 12,
    "timestamp": 123456779
}
```

This results in two delta messages:

```json
{
    "state": {
        "color": "RED"
    },
    "version": 11,
    "timestamp": 123456778
}
```
Trim Shadow Messages

The device might receive these messages out of order. Because the state in these messages is cumulative, a device can safely discard any messages that contain a version number older than the one it is tracking. If the device receives the delta for version 12 before version 11, it can safely discard the version 11 message.

To reduce the size of shadow messages sent to your device, define a rule that selects only the fields your device needs then republishes the message on an MQTT topic to which your device is listening.

The rule is specified in JSON and should look like the following:

```json
{
    "sql": "SELECT state, version FROM '##aws/things/+/shadow/update/delta'",
    "ruleDisabled": false,
    "actions": [{
        "republish": {
            "topic": "${topic(2)}/delta",
            "roleArn": "arn:aws:iam::123456789012:role/my-iot-role"
        }
    }]
}
```

The SELECT statement determines which fields from the message will be republished to the specified topic. A "+" wild card is used to match all shadow names. The rule specifies that all matching messages should be republished to the specified topic. In this case, the "\$(topic())" function is used to specify the topic on which to republish. \$(topic(2)) evaluates to the thing name in the original topic. For more information about creating rules, see Rules.

Device Shadow RESTful API

A shadow exposes the following URI for updating state information:

```
https://endpoint/things/thingName/shadow
```

The endpoint is specific to your AWS account. To retrieve your endpoint, use the describe-endpoint command. The format of the endpoint is as follows:

```
identifier.iot.region.amazonaws.com
```

API Actions

- GetThingShadow (p. 269)
- UpdateThingShadow (p. 269)
• DeleteThingShadow (p. 270)

GetThingShadow

Gets the shadow for the specified thing.

The response state document includes the delta between the desired and reported states.

Request

The request includes the standard HTTP headers plus the following URI:

HTTP GET https://endpoint/things/thingName/shadow

Response

Upon success, the response includes the standard HTTP headers plus the following code and body:

HTTP 200
BODY: response state document

For more information, see Example Response State Document (p. 277).

Authorization

Retrieving a shadow requires a policy that allows the caller to perform the iot:GetThingShadow action. The Device Shadow service accepts two forms of authentication: Signature Version 4 with IAM credentials or TLS mutual authentication with a client certificate.

The following is an example policy that allows a caller to retrieve a device's shadow:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "iot:GetThingShadow",
    "Resource": ["arn:aws:iot:region:account:thing/thing"]
  }]
}
```

UpdateThingShadow

Updates the shadow for the specified thing.

Updates affect only the fields specified in the request state document. Any field with a value of null is removed from the device's shadow.

Request

The request includes the standard HTTP headers plus the following URI and body:

HTTP POST https://endpoint/things/thingName/shadow
BODY: request state document

For more information, see Example Request State Document (p. 277).

Response
Upon success, the response includes the standard HTTP headers plus the following code and body:

```
HTTP 200
BODY: response state document
```

For more information, see Example Response State Document (p. 277).

**Authorization**

Updating a shadow requires a policy that allows the caller to perform the `iot:UpdateThingShadow` action. The Device Shadow service accepts two forms of authentication: Signature Version 4 with IAM credentials or TLS mutual authentication with a client certificate.

The following is an example policy that allows a caller to update a device's shadow:

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": "iot:UpdateThingShadow",
      "Resource": ["arn:aws:iot:region:account:thing/thing"]
   }]
}
```

---

**DeleteThingShadow**

Deletes the shadow for the specified thing.

**Request**

The request includes the standard HTTP headers plus the following URI:

```
HTTP DELETE https://endpoint/things/thingName/shadow
```

**Response**

Upon success, the response includes the standard HTTP headers plus the following code and body:

```
HTTP 200
BODY: Empty response state document
```

**Authorization**

Deleting a device's shadow requires a policy that allows the caller to perform the `iot:DeleteThingShadow` action. The Device Shadow service accepts two forms of authentication: Signature Version 4 with IAM credentials or TLS mutual authentication with a client certificate.

The following is an example policy that allows a caller to delete a device's shadow:

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": "iot:DeleteThingShadow",
      "Resource": ["arn:aws:iot:region:account:thing/thing"]
   }]
}
```
Shadow MQTT Topics

The Device Shadow service uses reserved MQTT topics to enable applications and devices to get, update, or delete the state information for a device (shadow). The names of these topics start with $aws/things/thingName/shadow. Publishing and subscribing on shadow topics requires topic-based authorization. AWS IoT reserves the right to add new topics to the existing topic structure. For this reason, we recommend that you avoid wild card subscriptions to shadow topics. For example, avoid subscribing to topic filters like $aws/things/thingName/shadow/# because the number of topics that match this topic filter might increase as AWS IoT introduces new shadow topics. For examples of the messages published on these topics see Device Shadow Service Data Flow (p. 249).

The following are the MQTT topics used for interacting with shadows.

**Topics**

- /update (p. 271)
- /update/accepted (p. 272)
- /update/documents (p. 272)
- /update/rejected (p. 273)
- /update/delta (p. 273)
- /get (p. 274)
- /get/accepted (p. 274)
- /get/rejected (p. 275)
- /delete (p. 275)
- /delete/accepted (p. 276)
- /delete/rejected (p. 276)

**/update**

Publish a request state document to this topic to update the device’s shadow:

```
$aws/things/thingName/shadow/update
```

A client attempting to update the state of a thing would send a JSON request state document like this:

```
{
  "state" : {
    "desired" : {
      "color" : "red",
      "power" : "on"
    }
  }
}
```

A device updating its shadow would send a JSON request state document like this:

```
{
  "state" : {
    "reported" : {
      "color" : "red",
      "power" : "on"
    }
  }
}
```
AWS IoT responds by publishing to either /update/accepted (p. 272) or /update/rejected (p. 273).

For more information, see Request State Documents (p. 277).

**Example Policy**

The following is an example of the required policy:

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["iot:Publish"],
    }]
}
```

### /update/accepted

AWS IoT publishes a response state document to this topic when it accepts a change for the device's shadow:

`$aws/things/thingName/shadow/update/accepted`

For more information, see Response State Documents (p. 277).

**Example Policy**

The following is an example of the required policy:

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["iot:Subscribe", "iot:Receive"],
    }]
}
```

### /update/documents

AWS IoT publishes a state document to this topic whenever an update to the shadow is successfully performed:

`$aws/things/thingName/shadow/update/documents`

The JSON document will contain two primary nodes: previous and current. The previous node will contain the contents of the full shadow document before the update was performed while current will contain the full shadow document after the update is successfully applied. When the shadow is updated (created) for the first time, the previous node will contain null.
Example Policy

The following is an example of the required policy:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iot:Subscribe",
            "iot:Receive"
        ],
    }]
}
```

/update/rejected

AWS IoT publishes an error response document to this topic when it rejects a change for the device's shadow:

```
/aws/things/thingName/shadow/update/rejected
```

For more information, see Error Response Documents (p. 278).

Example Policy

The following is an example of the required policy:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iot:Subscribe",
            "iot:Receive"
        ],
    }]
}
```

/update/delta

AWS IoT publishes a response state document to this topic when it accepts a change for the device's shadow and the request state document contains different values for desired and reported states:

```
/aws/things/thingName/shadow/update/delta
```

For more information, see Response State Documents (p. 277).

Publishing Details

- A message published on update/delta includes only the desired attributes that differ between the desired and reported sections. It contains all of these attributes, regardless of whether these
attributes were contained in the current update message or were already stored in AWS IoT. Attributes that do not differ between the desired and reported sections are not included.

- If an attribute is in the reported section but has no equivalent in the desired section, it is not included.
- If an attribute is in the desired section but has no equivalent in the reported section, it is included.
- If an attribute is deleted from the reported section but still exists in the desired section, it is included.

Example Policy

The following is an example of the required policy:

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iot:Subscribe",
            "iot:Receive"
        ],
    }]
}
```

/get

Publish an empty message to this topic to get the device's shadow:

`#aws/things/thingName/shadow/get`

AWS IoT responds by publishing to either /get/accepted (p. 274) or /get/rejected (p. 275).

Example Policy

The following is an example of the required policy:

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iot:Publish"
        ],
    }]
}
```

/get/accepted

AWS IoT publishes a response state document to this topic when returning the device's shadow:

`#aws/things/thingName/shadow/get/accepted`

For more information, see Response State Documents (p. 277).
Example Policy

The following is an example of the required policy:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iot:Subscribe",
                "iot:Receive"
            ],
            "Resource": ["arn:aws:iot:region:account:topicfilter/$aws/things/thingName/shadow/get/accepted"]
        }
    ]
}
```

/get/rejected

AWS IoT publishes an error response document to this topic when it can't return the device's shadow:

`$aws/things/thingName/shadow/get/rejected`

For more information, see Error Response Documents (p. 278).

Example Policy

The following is an example of the required policy:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iot:Subscribe",
                "iot:Receive"
            ],
        }
    ]
}
```

/delete

To delete a device's shadow, publish an empty message to the delete topic:

`$aws/things/thingName/shadow/delete`

The content of the message is ignored.

AWS IoT responds by publishing to either /delete/accepted (p. 276) or /delete/rejected (p. 276).

Example Policy

The following is an example of the required policy:

```json
{
```

275
"Version": "2012-10-17",
"Statement": [{
  "Effect": "Allow",
  "Action": [
    "iot:Subscribe",
    "iot:Receive"
  ],
  ]
}]

/delete/accepted

AWS IoT publishes a message to this topic when a device's shadow is deleted:

$aws/things/thingName/shadow/delete/accepted

Example Policy

The following is an example of the required policy:

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "iot:Subscribe",
      "iot:Receive"
    ],
    "Resource": ["arn:aws:iot:region:account:topicfilter/$aws/things/thingName/shadow/delete/accepted"
    ]
  }]
}

/delete/rejected

AWS IoT publishes an error response document to this topic when it can't delete the device's shadow:

$aws/things/thingName/shadow/delete/rejected

For more information, see Error Response Documents (p. 278).

Example Policy

The following is an example of the required policy:

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "iot:Subscribe",
      "iot:Receive"
    ],
    ]
  }]
}
Shadow Document Syntax

The Device Shadow service uses the following documents in UPDATE, GET, and DELETE operations using the RESTful API (p. 268) or MQTT Pub/Sub Messages (p. 271). For more information, see Device Shadow Service Documents (p. 256).

Examples

- Request State Documents (p. 277)
- Response State Documents (p. 277)
- Error Response Documents (p. 278)

Request State Documents

Request state documents have the following format:

```json
{
    "state": {
        "desired": {
            "attribute1": integer2,
            "attribute2": "string2",
            ...
            "attributeN": boolean2
        },
        "reported": {
            "attribute1": integer1,
            "attribute2": "string1",
            ...
            "attributeN": boolean1
        }
    }
    "clientToken": "token",
    "version": version
}
```

- **state** — Updates affect only the fields specified.
- **clientToken** — If used, you can verify that the request and response contain the same client token.
- **version** — If used, the Device Shadow service processes the update only if the specified version matches the latest version it has.

Response State Documents

Response state documents have the following format:

```json
{
    "state": {
        "desired": {
            "attribute1": integer2,
            "attribute2": "string2",
            ...
            "attributeN": boolean2
        }
    }
}
```
Error Response Documents

Error response documents have the following format:

```json
{
  "state": {
    "reported": {
      "attribute1": integer1,
      "attribute2": "string1",
      ...
      "attributeN": boolean1
    },
    "delta": {
      "attribute3": integerX,
      "attribute5": "stringY"
    }
  },
  "metadata": {
    "desired": {
      "attribute1": {
        "timestamp": timestamp
      },
      "attribute2": {
        "timestamp": timestamp
      },
      ...
      "attributeN": {
        "timestamp": timestamp
      }
    },
    "reported": {
      "attribute1": {
        "timestamp": timestamp
      },
      "attribute2": {
        "timestamp": timestamp
      },
      ...
      "attributeN": {
        "timestamp": timestamp
      }
    }
  },
  "timestamp": timestamp,
  "clientToken": "token",
  "version": version
}
```

- **state**
  - **reported** — Only present if a thing reported any data in the reported section and contains only fields that were in the request state document.
  - **desired** — Only present if a thing reported any data in the desired section and contains only fields that were in the request state document.
  - **metadata** — Contains the timestamps for each attribute in the desired and reported sections so that you can determine when the state was updated.
  - **timestamp** — The Epoch date and time the response was generated by AWS IoT.
  - **clientToken** — Present only if a client token was used when publishing valid JSON to the /update topic.
  - **version** — The current version of the document for the device's shadow shared in AWS IoT. It is increased by one over the previous version of the document.

Error Response Documents

Error response documents have the following format:
Shadow Error Messages

The Device Shadow service publishes a message on the error topic (over MQTT) when an attempt to change the state document fails. This message is only emitted as a response to a publish request on one of the reserved $aws topics. If the client updates the document using the REST API, then it receives the HTTP error code as part of its response, and no MQTT error messages are emitted.

<table>
<thead>
<tr>
<th>HTTP Error Code</th>
<th>Error Messages</th>
</tr>
</thead>
</table>
| 400 (Bad Request) | • Invalid JSON  
|                 | • Missing required node: state  
|                 | • State node must be an object  
|                 | • Desired node must be an object  
|                 | • Reported node must be an object  
|                 | • Invalid version  
|                 | • Invalid clientToken  
|                 | **Note**  
|                 | A client token that is longer than 64 bytes will cause this response.  
|                 | • JSON contains too many levels of nesting; maximum is 6  
|                 | • State contains an invalid node  
| 401 (Unauthorized) | • Unauthorized  
| 403 (Forbidden) | • Forbidden  
| 404 (Not Found) | • Thing not found  
| 409 (Conflict) | • Version conflict  
| 413 (Payload Too Large) | • The payload exceeds the maximum size allowed  
| 415 (Unsupported Media Type) | • Unsupported documented encoding; supported encoding is UTF-8  
<p>| 429 (Too Many Requests) | • The Device Shadow service will generate this error message when there are more than 10 in-flight requests. |</p>
<table>
<thead>
<tr>
<th>HTTP Error Code</th>
<th>Error Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>500 (Internal Server Error)</td>
<td>• Internal service failure</td>
</tr>
</tbody>
</table>
Jobs

AWS IoT jobs can be used to define a set of remote operations that are sent to and executed on one or more devices connected to AWS IoT.

Jobs Key Concepts

job

A job is a remote operation that is sent to and executed on one or more devices connected to AWS IoT. For example, you can define a job that instructs a set of devices to download and install application or firmware updates, reboot, rotate certificates, or perform remote troubleshooting operations.

job document

To create a job, you must first create a job document that is a description of the remote operations to be performed by the devices.

Job documents are UTF-8 encoded JSON documents and should contain any information your devices need to perform a job. A job document will most likely contain one or more URLs where the device can download an update or some other data. The job document itself can be stored in an Amazon S3 bucket, or be included inline with the command that creates the job.

target

When you create a job, you specify a list of targets that are the devices that should perform the operations. The targets can be things or thing groups (p. 109) or both. AWS IoT Jobs sends a message to each target to inform it that a job is available.

job execution

A job execution is an instance of a job on a target device. The target starts an execution of a job by downloading the job document. It then performs the operations the document specifies, and reports its progress to AWS IoT. An execution number is a unique identifier of a specific job execution on a specific target. The Jobs service provides commands to track the progress of a job execution on a specific target and the progress of a job generally across all the targets of the job.

snapshot job

By default, a job is sent to all targets that you specify when you create the job. After those targets complete the job (or report that they are unable to do so), the job is complete.

continuous job

A continuous job is sent to all targets that you specify when you create the job, but continues to run and will be sent to any new devices (things) that are added to the target group. For example, a continuous job can be used to onboard or upgrade devices as they are added to a group. You can make a job continuous by setting an optional parameter when you create the job.

rollouts

When you create a job you can specify how quickly targets are notified of a pending job execution. This allows you to create a staged rollout to better manage updates, reboots, and other operations.

The following field can be added to the CreateJob request to specify the maximum number of targets that will be informed of the job per minute:
presigned URLs

To allow a device secure, time-limited access to data beyond that included in the job document itself, you can use presigned Amazon S3 URLs. You can place your data in an Amazon S3 bucket and add a placeholder link to the data in the job document. When the Jobs service receives a request for the job document, it parses the job document looking for placeholder links and it replaces them with presigned Amazon S3 URLs.

The placeholder link is of the following form:

`${aws:iot:s3-presigned-url:https://s3.amazonaws.com/bucket/key}`

where `bucket` is your bucket name and `key` is the object in the bucket to which you are linking.

Managing Jobs

Jobs are created and managed using the Jobs HTTPS API, the AWS Command Line Interface or the AWS SDKs. For more information on these tools, see Job Management and Control API (p. 304), AWS CLI Command Reference: iot or AWS SDKs and Tools.

Create Jobs

CreateJob

You use the `CreateJob` command to create a job. The job is queued for execution on the targets (things or thing groups) that you specify. To create a job, you need a job document that can be included in the body of the request or as a link to an Amazon S3 document. If the job includes downloading files using presigned Amazon S3 URLs, you need an IAM role ARN that has permission to download the file and grants permission to AWS IoT to assume the role.

If you have a file called `job-document.json` stored in an Amazon S3 bucket called `jobBucket` and the role with permission to download files from Amazon S3 is called `S3DownloadRole`, the CLI command to create a job would look like this:

```bash
aws iot create-job  
--job-id 010  
--targets arn:aws:iot:us-east-1:123456789012:thing/thingOne  
--presigned-url-config 
"{"roleArn":": arn:aws:iam::123456789012:role/S3DownloadRole":, 
"expiresInSec":3600}"
```

If you want to specify the job document inline, use the `--document` parameter instead of the `--document-source` parameter.

A job is sent to and executed on targets in the order they appear in the `--targets` list. For example, if the targets list is:

```
[ arn:aws:iot:us-east-1:123456789012:thing/thingOne, 
  arn:aws:iot:us-east-1:123456789012:thinggroup/thinggroupOne, 
  arn:aws:iot:us-east-1:123456789012:thing/thingTwo,
```
then the job will be executed on thingOne, followed by the things in thinggroupOne, then thingTwo, and finally by the things in thinggroupTwo.

**Note**

Job documents that are specified as Amazon S3 files are retrieved at the time you create the job. Changing the contents of the Amazon S3 file you used as the source of your job document after you have created the job does not change what is sent to the targets of the job.

**granting permissions**

When creating a job that uses presigned Amazon S3 URLs, you must provide an IAM role ARN that grants permission to download files from the Amazon S3 bucket where the data or updates are stored. The role must also grant permission for AWS IoT to assume the role.

**To grant Jobs permission to assume your role:**

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Roles.
3. Search for your role and choose it.
4. Choose the Trust Relationships tab.
5. Choose the Edit Trust Relationship button.
6. On the Edit Trust Relationship page, replace the policy document with the following JSON:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": ["iot.amazonaws.com"
      ],
      "Action": "sts:AssumeRole"
    }
  ]
}
```

7. Choose Update Trust Policy.
8. If your job uses a job document that is an Amazon S3 object, choose Permissions and add a policy that grants permission to download files from your Amazon S3 bucket with the following JSON:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::your_S3_bucket/*"
    }
  ]
}
```
You can optionally specify a timeout for the presigned URL. For more information, see CreateJob (p. 317).

Cancel a Job

CancelJob

You use the the CancelJob command to cancel a job. Cancelling a job will stop AWS IoT rolling out any new job executions for the job. It will also cancel any job executions that have already been QUEUED. IoT will leave any job executions in a terminal state untouched because the device has already completed the job. If a job execution is IN_PROGRESS, it will also remain untouched unless you use the optional --force parameter.

```bash
aws iot cancel-job --job-id 010
```

The command displays no output.

When you cancel a job, job executions that are QUEUED will be canceled. Job executions that are IN_PROGRESS will be canceled if you specify the optional --force parameter. Job executions in a terminal state are not canceled.

**Warning**

Canceling a job that is IN_PROGRESS (by setting the --force parameter) will cancel any job executions that are IN_PROGRESS and cause the device that is executing the job to be unable to update the job execution status. Use caution and ensure that each device executing a job that is canceled is able to recover to a valid state.

The status of a canceled job or of one of its job executions is eventually consistent — IoT will stop scheduling new job executions and not present QUEUED job executions for that job to devices as soon as possible. But changing the status of a job execution to CANCELED may take some time depending on the number of devices and other factors.

Cancel a Job Execution

CancelJobExecution

You use the the CancelJobExecution command to cancel a job execution on a particular device. It will cancel a job execution that is QUEUED. If you want to cancel a job execution that is IN_PROGRESS, you must use the --force parameter.

```bash
aws iot cancel-job-execution --job-id 010 --thing-name myThing
```

The command displays no output.

A job execution that is QUEUED will be canceled. A job execution that is IN_PROGRESS will be canceled if you specify the optional --force parameter. Job executions in a terminal state cannot be canceled.

**Warning**

Canceling a job execution that is IN_PROGRESS will cause the device to be unable to update the job execution status. Use caution and ensure that the device is able to recover to a valid state.
This command will cause an InvalidStateTransitionException if the job execution is in a terminal state or if the job execution is IN_PROGRESS and the --force parameter is not set to true.

The status of a canceled job execution is eventually consistent — changing the status of a job execution to CANCELED may take some time depending various factors.

## Delete a Job

### DeleteJob

You use the the `DeleteJob` command to delete a job and its related job executions. By default, you can only delete a job which is in a terminal state ("COMPLETED" or "CANCELED") otherwise an exception will occur. However, if the `force` parameter is set to true, you can delete a job which is "IN_PROGRESS".

```bash
aws iot delete-job --job-id 010 --force|--no-force
```

The command displays no output.

**Warning**

Deleting a job which is "IN_PROGRESS", will cause a device which is executing the job to be unable to access job information or update the job execution status. Use caution and ensure that each device executing a job which is deleted is able to recover to a valid state.

Deleting a job may take some time, depending on the number of job executions created for the job and various other factors. While the job is being deleted, the status of the job will be shown as "DELETION_IN_PROGRESS". Attempting to delete or cancel a job whose status is already "DELETION_IN_PROGRESS" will result in an error.

Only 10 jobs may have status "DELETION_IN_PROGRESS" at the same time, or a LimitExceededException will occur.

## Get a Job Document

### GetJobDocument

You use the `GetJobDocument` command to retrieve a job document for a job. A job document is a description of the remote operations to be performed by the devices.

```bash
aws iot get-job-document --job-id 010
```

The command returns the job document for the specified job:

```json
{
    "document": "{"\n    "operation": "install",
    "url": "http://amazon.com/firmWareUpdate-01",
    "data": "$(aws:iot:s3-presigned-url:https://s3.amazonaws.com/job-test-bucket/datafile)"
}
```

**Note**

When you retrieve a job document using this command, any placeholder URLs are not replaced by presigned Amazon S3 URLs. The placeholder URLs are replaced by...
presigned Amazon S3 URLs in the job document that is returned when a device calls the GetPendingJobExecutions (p. 350) MQTT API.

List Jobs

You use the `ListJobs` command to get a list of all jobs in your AWS account. Note that job data and job execution data will be purged after 90 days.

more info (6)

```bash
aws iot list-jobs
```

The command lists all jobs in your account sorted by the job status:

```json
{
  "jobs": [
    {
      "status": "IN_PROGRESS",
      "lastUpdatedAt": 1486687079.743,
      "jobArn": "arn:aws:iot:us-east-1:123456789012:job/013",
      "createdAt": 1486687079.743,
      "targetSelection": "SNAPSHOT",
      "jobId": "013"
    },
    {
      "status": "COMPLETED",
      "lastUpdatedAt": 1486685868.444,
      "jobArn": "arn:aws:iot:us-east-1:123456789012:job/012",
      "createdAt": 1486685868.444,
      "completedAt": 148668789.690,
      "targetSelection": "SNAPSHOT",
      "jobId": "012"
    },
    {
      "status": "CANCELED",
      "lastUpdatedAt": 1486678850.575,
      "jobArn": "arn:aws:iot:us-east-1:123456789012:job/011",
      "createdAt": 1486678850.575,
      "targetSelection": "SNAPSHOT",
      "jobId": "011"
    }
  ]
}
```

Describe a Job

You use the `DescribeJob` command to get the status of a specific job.

more info (7)

```bash
# aws iot describe-job --job-id 010
```

The command returns the status of the specified job. For example:

```json
{
  "status": "CANCELED",
  "lastUpdatedAt": 1486678850.575,
  "jobArn": "arn:aws:iot:us-east-1:123456789012:job/011",
  "createdAt": 1486678850.575,
  "targetSelection": "SNAPSHOT",
  "jobId": "011"
}
```
List Executions for a Job

A job running on a specific device is represented by a job execution object. You use the `ListJobExecutionsForJob` command to list all job executions for a job.

The command returns a list of job executions:

```json
{
  "executionSummaries": [
    {
      "thingArn": "arn:aws:iot:us-east-1:123456789012:thing/thingOne",
      "jobExecutionSummary": {
        "status": "QUEUED",
        "lastUpdatedAt": 1486593196.378,
        "queuedAt": 1486593196.378,
        "executionNumber": 1234567890
      }
    },
    {
      "thingArn": "arn:aws:iot:us-east-1:123456789012:thing/thingTwo",
      "jobExecutionSummary": {
        "status": "IN_PROGRESS",
        "lastUpdatedAt": 1486593345.659,
        "executionNumber": 1234567890
      }
    }
  ]
}
```
You use the `ListJobExecutionsForThing` command to list all job executions running on a thing. The command returns a list of job executions that are running or have run on the specified thing:

```json
{
    "executionSummaries": [
    {
        "jobExecutionSummary": {
            "status": "QUEUED",
            "lastUpdatedAt": 1486687082.071,
            "queuedAt": 1486687082.071,
            "executionNumber": 9876543210
        },
        "jobId": "013"
    },
    {
        "jobExecutionSummary": {
            "status": "IN_PROCESS",
            "startAt": 1486685870.729,
            "lastUpdatedAt": 1486685870.729,
            "queuedAt": 1486685870.729,
            "executionNumber": 1357924680
        },
        "jobId": "012"
    },
    {
        "jobExecutionSummary": {
            "status": "COMPLETED",
            "startAt": 1486678853.415,
            "lastUpdatedAt": 1486678853.415,
            "queuedAt": 1486678853.415,
            "executionNumber": 4357680912
        },
        "jobId": "011"
    },
    {
        "jobExecutionSummary": {
            "status": "CANCELED",
            "startAt": 1486593196.378,
            "lastUpdatedAt": 1486593196.378,
            "queuedAt": 1486593196.378,
            "executionNumber": 2143174250
        },
        "jobId": "010"
    }
    ]
}
```
Describe Job Execution

You use the `DescribeJobExecution` command to get the status of a specific job execution. You specify a job ID and thing name (and, optionally, an execution number) to identify the job execution. The job's execution status must be `QUEUED` or `IN_PROGRESS`.

```
aws iot describe-job-execution --job-id 017 --thing-name thingOne
```

The command returns the `JobExecution` (p. 307). For example:

```
{
   "execution": {
      "jobId": "017",
      "executionNumber": 4516820379,
      "thingArn": "arn:aws:iot:us-east-1:123456789012:thing/thingOne",
      "versionNumber": 123,
      "createdAt": 1489084805.285,
      "lastUpdatedAt": 1489086279.937,
      "startedAt": 1489086279.937,
      "status": "IN_PROGRESS",
      "statusDetails": {
         "status": "IN_PROGRESS",
         "detailsMap": {
            "percentComplete": "10"
         }
      }
   }
}
```

Delete Job Execution

You use the `DeleteJobExecution` command to delete a specific job execution. You must specify a job ID and a thing name and, optionally, an execution number to identify the job execution.

```
aws iot delete-job-execution --job-id 017 --thing-name thingOne --execution-number 1234567890 --force|--no-force
```

The command displays no output.

By default, the job execution must be "QUEUED" or in a terminal state (SUCCEEDED, FAILED, REJECTED, REMOVED or CANCELED) or an error will occur. Otherwise, you can set the `force` parameter to true to delete a job execution `IN_PROGRESS`.

**Warning**
Deleting a job execution which is "IN_PROGRESS", will cause the device which is executing the job to be unable to access job information or update the job execution status. Use caution and ensure that the device is able to recover to a valid state.
Jobs Events

AWS IoT Jobs publishes MQTT messages to reserved topics when jobs are completed, canceled, or deleted, and when a device reports success or failure when executing a job.

Because job cancellation and deletion may take some time, two messages are sent to indicate the start and end of a request. For example, when a cancellation request starts, a message is sent to the $aws/events/job/jobID/cancellation_in_progress topic; and when the cancellation request completes, a message is sent to the $aws/events/job/jobID/canceled topic. A similar process occurs for a job deletion request. Management and monitoring applications can keep track of the status of jobs by subscribing to these topics.

For more information about publishing and subscribing to MQTT topics, see Message Broker for AWS IoT (p. 165)

job completed/canceled/deleted/cancellation_in_progress/deletion_in_progress

AWS IoT Jobs publishes a message on an MQTT topic when a job is completed, canceled, and deleted:

- $aws/events/job/jobID/completed
- $aws/events/job/jobID/canceled
- $aws/events/job/jobID/deleted
- $aws/events/job/jobID/cancellation_in_progress
- $aws/events/job/jobID/deletion_in_progress

more info (12)

The "completed" message contains the following example payload:

```json
{
  "eventType": "JOB",
  "eventId": "7364f8d1-8b65-4824-85d5-6c14686c97c6",
  "timestamp": 1234567890,
  "operation": "completed",
  "jobId": "27450507-bf6f-4012-92af-bb8a1c8c4484",
  "status": "COMPLETED",
  "targetSelection": "SNAPSHOT|CONTINUOUS",
  "targets": [
    "arn:aws:iot:us-east-1:123456789012:thing/a39f6f91-70cf-4bd2-a381-9c66df1a80d0",
    "arn:aws:iot:us-east-1:123456789012:thinggroup/2fc4c0a4-6e45-4525-a239-0fe8d3dd21bb"
  ],
  "description": "My Job Description",
  "completedAt": 1234567890123,
  "createdAt": 1234567890123,
  "lastUpdatedAt": 1234567890123,
  "comment": "Comment for this operation",
  "jobProcessDetails": {
    "numberOfCanceledThings": 0,
    "numberOfRejectedThings": 0,
    "numberOfFailedThings": 0,
    "numberOfRemovedThings": 0,
    "numberOfSucceededThings": 3
  }
}
```

The "canceled" message contains the following example payload:

```json
```
The "deleted" message contains the following example payload:

```json
{
    "eventType": "JOB",
    "eventId": "568d2ade-2e9c-46e6-a115-18afa1286b06",
    "timestamp": 1234567890,
    "operation": "deleted",
    "jobId": "4d2a531a-da2e-47bb-8b9e-ff5adcd53ef0",
    "status": "DELETED",
    "targetSelection": "SNAPSHOT|CONTINUOUS",
    "targets": [
        "arn:aws:iot:us-east-1:123456789012:thing/Thing0-947b9c0c-ff10-4a80-b4b3-cd33d0145a0f",
        "arn:aws:iot:us-east-1:123456789012:thinggroup/ThingGroup1-95c644d5-1621-41a6-9aa5-ad2de581d18f"
    ],
    "description": "My job description",
    "createdAt": 1234567890123,
    "lastUpdatedAt": 1234567890123,
    "comment": "Comment for this operation",
    "jobProcessDetails": {
        "numberOfCanceledThings": 0,
        "numberOfRejectedThings": 0,
        "numberOfFailedThings": 0,
        "numberOfRemovedThings": 0,
        "numberOfSucceededThings": 3
    }
}
```

The "cancellation_in_progress" message contains the following example payload:

```json
{
    "eventType": "JOB",
    "eventId": "568d2ade-2e9c-46e6-a115-18afa1286b06",
    "timestamp": 1234567890,
    "operation": "cancellation_in_progress",
    "jobId": "4d2a531a-da2e-47bb-8b9e-ff5adcd53ef0",
    "status": "CANCELLATION_IN_PROGRESS",
    "targetSelection": "SNAPSHOT|CONTINUOUS",
    "targets": [
        "arn:aws:iot:us-east-1:123456789012:thing/Thing0-947b9c0c-ff10-4a80-b4b3-cd33d0145a0f",
        "arn:aws:iot:us-east-1:123456789012:thinggroup/ThingGroup1-95c644d5-1621-41a6-9aa5-ad2de581d18f"
    ],
    "description": "My job description",
    "createdAt": 1234567890123,
    "lastUpdatedAt": 1234567890123,
    "comment": "Comment for this operation"
}
```
The "deletion_in_progress" message contains the following example payload:

```json
{
    "eventType": "JOB",
    "eventId": "568d2a9e-2e9c-46e6-a115-18afa1286b06",
    "timestamp": 1234567890,
    "operation": "deletion_in_progress",
    "jobId": "4d2a531a-da2e-47bb-8b9e-ff5adcd53ef0",
    "status": "DELETION_IN_PROGRESS",
    "targetSelection": "SNAPSHOT|CONTINUOUS",
    "targets": [
        "arn:aws:iot:us-east-1:123456789012:thing/Thing0-947b9c0c-ff10-4a80-b4b3-cd33d0145a0f",
        "arn:aws:iot:us-east-1:123456789012:thinggroup/ThingGroup1-95c644d5-1621-41a6-9aa5-ad2de581d18f"
    ],
    "description": "My job description",
    "createdAt": 1234567890123,
    "lastUpdatedAt": 1234567890123,
    "comment": "Comment for this operation"
}
```

job execution terminal status

AWS IoT Jobs publishes a message when a device updates a job execution to terminal status:

- `$aws/events/jobExecution/jobID/succeeded`
- `$aws/events/jobExecution/jobID/failed`
- `$aws/events/jobExecution/jobID/rejected`
- `$aws/events/jobExecution/jobID/canceled`
- `$aws/events/jobExecution/jobID/removed`
- `$aws/events/jobExecution/jobID/deleted`

more info (13)

The message contains the following example payload:

```json
{
    "eventType": "JOB_EXECUTION",
    "eventId": "cca89fa5-8a7f-4ced-8c20-5e653af3b3572",
    "timestamp": 1234567890,
    "operation": "succeeded|failed|rejected|canceled|removed|deleted",
    "jobId": "154b39e5-60b0-48a4-9b73-f6f8dd032d27",
    "thingArn": "arn:aws:iot:us-east-1:123456789012:myThing/6d639fbc-8f85-4a90-924d-a2867f8366a7",
    "status": "SUCCEEDED|FAILED|REJECTED|CANCELED|REMOVED|DELETED",
    "statusDetails": {
        "key": "value"
    }
}
```
Note
When a job has been deleted, the operation field in the message will show this, but the status field will reflect what the job execution status was prior to the deletion.

Devices and Jobs
device communication with Jobs

Devices can communicate with Jobs through one of three methods:

- MQTT
- HTTP SigV4
- HTTP TLS

using the MQTT protocol

Communication between the Jobs service and your devices can occur over the MQTT protocol. Devices subscribe to MQTT topics to be notified of new jobs and to receive responses from the Jobs service. Devices publish on MQTT topics to query or update the state of a job execution. Each device has its own general MQTT topic. For more information about publishing and subscribing to MQTT topics, see Message Broker for AWS IoT (p. 165)

Note
You must use the correct endpoint when communicating with Jobs via MQTT. To find it, use the DescribeEndpoint command. For example, using the CLI:

```
aws iot describe-endpoint --endpoint-type iot:Data
```

you will get a result similar to:

```
{
    "endpointAddress": "a1b2c3d4e5f6g7.iot.us-west-2.amazonaws.com"
}
```

With this method, your device uses its device-specific certificate and private key to authenticate with the Jobs service.

Devices can:

- Be notified whenever a job execution is added or removed from the list of pending job executions for a device by subscribing to the $aws/things/thing-name/jobs/notify MQTT topic, where thing-name is the name of the thing associated with the device.
- Be notified when the next pending job execution has changed by subscribing to the $aws/things/thing-name/jobs/notify-next MQTT topic, where thing-name is the name of the thing associated with the device.
- Update the status of a job execution by calling the UpdateJobExecution (p. 362) API.
- Query the status of a job execution by calling the DescribeJobExecution (p. 358) API.
- Retrieve a list of pending job executions by calling the GetPendingJobExecutions (p. 350) API.
- Retrieve the next pending job execution by calling the DescribeJobExecution (p. 358) API with jobId $next.
- Get and start the next pending job execution by calling the StartNextPendingJobExecution (p. 353) API.
The Jobs service publishes success and failure messages on an MQTT topic formed by appending `accepted` or `rejected` to the topic used to make the request. For example, if a request message is published on the `$aws/things/myThing/jobs/get` topic, the Jobs service publishes success messages on the `$aws/things/myThing/jobs/get/accepted` topic and publishes rejected messages on the `$aws/things/myThing/jobs/get/rejected` topic.

**using HTTP SigV4**

Communication between the Jobs service and your devices can occur over HTTP SigV4 on port 443. This is the method used by the AWS SDKs and CLI. For more information about those tools, see [AWS CLI Command Reference: iot-jobs-data](https://docs.aws.amazon.com/iot/latest/developerguide/aws-cli-iot-jobs-data.html) or AWS SDKs and Tools and refer to the `IotJobsDataPlane` section for your preferred language.

**Note**

You must use the correct endpoint when communicating with Jobs via HTTP SigV4 or using an AWS SDK or CLI `IotJobsDataPlane` command. To find it, use the `DescribeEndpoint` command. For example, using the CLI:

```
aws iot describe-endpoint --endpoint-type iot:Jobs
```

you will get a result similar to:

```
{
  "endpointAddress": "a1b2c3d4e5f6g7.jobs.iot.us-west-2.amazonaws.com"
}
```

With this method of communication, your device will use IAM credentials to authenticate with the Jobs service.

The following commands are available using this method:

- **DescribeJobExecution**
  
  `aws iot-jobs-data describe-job-execution ...`

- **GetPendingJobExecutions**
  
  `aws iot-jobs-data get-pending-job-executions ...`

- **StartNextPendingJobExecution**
  
  `aws iot-jobs-data start-next-pending-job-execution ...`

- **UpdateJobExecution**
  
  `aws iot-jobs-data update-job-execution ...`

**using HTTP TLS**

Communication between the Jobs service and your devices can occur over HTTP TLS on port 8443 using a third-party software client that supports this protocol.

**Note**

You must use the correct endpoint when communicating with Jobs via HTTP TLS. To find it, use the `DescribeEndpoint` command. For example, using the CLI:

```
aws iot describe-endpoint --endpoint-type iot:Jobs
```

you will get a result similar to:

```
{
```

The following commands are available using this method:

- **DescribeJobExecution**
  
  `aws iot-jobs-data describe-job-execution ...`

- **GetPendingJobExecutions**
  
  `aws iot-jobs-data get-pending-job-executions ...`

- **StartNextPendingJobExecution**
  
  `aws iot-jobs-data start-next-pending-job-execution ...`

- **UpdateJobExecution**
  
  `aws iot-jobs-data update-job-execution ...`
"endpointAddress": "a1b2c3d4e5f6g7.jobs.iot.us-west-2.amazonaws.com"
}

With this method, your device uses X509 certificate based authentication (for example, using its device-specific certificate and private key.)

The following commands are available using this method:

- DescribeJobExecution
- GetPendingJobExecutions
- StartNextPendingJobExecution
- UpdateJobExecution

Programming Devices to Work with Jobs

The examples in this section use MQTT to illustrate how a device works with Jobs. Alternatively, you could use the corresponding API or CLI commands if you want. For these examples, we assume a device called MyThing will subscribe to the following MQTT topics:

- $aws/things/MyThing/jobs/notify (or $aws/things/MyThing/jobs/notify-next)
- $aws/things/MyThing/jobs/get/accepted
- $aws/things/MyThing/jobs/get/rejected
- $aws/things/MyThing/jobs/jobId/get/accepted
- $aws/things/MyThing/jobs/jobId/get/rejected

Device Workflow

In general, there are two ways a device can handle the jobs it is given to execute.

Option A: Get the next job

1. When a device first comes online, it should subscribe to the device's notify-next topic.
2. Call the DescribeJobExecution (p. 358) MQTT API with jobId $next to get the next job, its job document, and other details, including any state saved in statusDetails.
3. Call the UpdateJobExecution (p. 362) MQTT API to update the job status. Or, to combine this and the previous step in one call, the device can call StartNextPendingJobExecution (p. 353).
4. Perform the actions specified by the job document using the UpdateJobExecution (p. 362) MQTT API to report on the progress of the job.
5. Continue to monitor the job execution by calling the DescribeJobExecution (p. 358) MQTT API with this jobId. If the job execution is canceled or deleted while the device is running the job, the device should be capable of recovering to a valid state.
6. Call the UpdateJobExecution (p. 362) MQTT API when finished with the job to update the job status and report success or failure.
7. Because this job's execution status has been changed to a terminal state, the next job available for execution (if any) will change. The device is notified that the next pending job execution has changed. At this point, the device should continue as described in step 2.

If the device remains online, it will continue to receive notifications of the next pending job execution, including its JobExecutionData, whenever it completes a job or when a new pending job execution is added. When this occurs, the device continues as described in step 2.
Option B: Pick from available jobs

1. When a device first comes online, it should subscribe to the thing’s notify topic.
2. Call the GetPendingJobExecutions (p. 350) MQTT API to get a list of pending job executions.
3. If the list contains one or more job executions, pick one.
4. Call the DescribeJobExecution (p. 358) MQTT API to get the job document and other details, including any state saved in statusDetails.
5. Call the UpdateJobExecution (p. 362) MQTT API to update the job status. If the includeJobDocument field is set to true in this command, the device can skip the previous step and retrieve the job document at this point.
6. Perform the actions specified by the job document using the UpdateJobExecution (p. 362) MQTT API to report on the progress of the job.
7. Continue to monitor the job execution by calling the DescribeJobExecution (p. 358) MQTT API with this jobId. If the job execution is canceled or deleted while the device is running the job, the device should be capable of recovering to a valid state.
8. Call the UpdateJobExecution (p. 362) MQTT API when finished with the job to update the job status and to report success or failure.

If the device remains online, it will be notified of all pending job executions whenever a new pending job execution becomes available. When this occurs, the device can continue as described in step 2.

If the device is unable to execute the job, it should call the UpdateJobExecution (p. 362) MQTT API to update the job status to REJECTED.

Starting a New Job

new job notification

When a new job is created, Jobs publishes a message on the $aws/things/thing-name/jobs/notify topic for each target device.

The message contains the following information:

```json
{
  "timestamp":1476214217017,
  "jobs":{
    "QUEUED":[
      {
        "jobId":"0001",
        "queuedAt":1476214216981,
        "lastUpdatedAt":1476214216981,
        "versionNumber": 1
      }
    ]
  }
}
```

The device receives this message on the '$aws/things/thingName/jobs/notify' topic when the job execution is queued.

get job information

To get more information about a job execution, the device calls the DescribeJobExecution (p. 358) MQTT API with the includeJobDocument field set to true.
If the request is successful, Jobs publishes a message on the $aws/things/MyThing/jobs/0023/get/accepted topic:

```json
{
    "clientToken": "client-001",
    "timestamp": 1489097434407,
    "execution": {
        "jobId": "023",
        "status": "QUEUED",
        "queuedAt": 1489097374841,
        "lastUpdatedAt": 1489097374841,
        "versionNumber": 1,
        "jobDocument": {
            "< contents of job document >"
        }
    }
}
```

**Note**

If the request fails, Jobs publishes a message on the $aws/things/MyThing/jobs/0023/get/rejected topic.

The device now has the job document, that it can interpret to perform the remote operations for the job. If the job document contains an Amazon S3 presigned URL, the device can use that URL to download any required files for the job.

### Report Job Execution Status

**update execution status**

As the device is executing the job, it can call the `UpdateJobExecution (p. 362)` MQTT API to update the status of the job execution. For example, a device can update the job execution status to **IN_PROGRESS** by publishing the following message on the $aws/things/MyThing/jobs/0023/update topic:

```json
{
    "status":"IN_PROGRESS",
    "statusDetails": {
        "progress": "50%"
    },
    "expectedVersion":"1",
    "clientToken":"client001"
}
```

Jobs responds by publishing a message to the $aws/things/MyThing/jobs/0023/update/accepted or $aws/things/MyThing/jobs/0023/update/rejected topic:

```json
{
    "clientToken":"client001",
    "timestamp":1476289222841
}
```

The device can combine the two previous requests by calling `StartNextPendingJobExecution (p. 353)`, that gets and starts the next pending job execution and
allows the device to update the job execution status. This request also returns the job document when there is a job execution pending.

The `status` field can be set to QUEUED, IN_PROGRESS, SUCCESS, FAILED, REJECTED, REMOVED, or CANCELED. You cannot update the status of a job execution that is already in a terminal state.

**Report execution completed**

When the device is finished executing the job, it calls the `UpdateJobExecution (p. 362)` MQTT API. If the job was successful, set `status` to SUCCESS and, in `statusDetails` in the message payload, add other information about the job as name/value pairs.

For example:

```json
{
  "status":"SUCCESS",
  "statusDetails": {
    "progress":"100%"
  },
  "expectedVersion":"2",
  "clientToken":"client-001"
}
```

If the job was not successful, set `status` to FAILED and, in `statusDetails`, add information about the error that occurred:

```json
{
  "status":"FAILED",
  "statusDetails": {
    "errorCode":"101",
    "errorMsg":"Unable to install update"
  },
  "expectedVersion":"2",
  "clientToken":"client-001"
}
```

**Note**
The `statusDetails` attribute can contain any number of name/value pairs.

When Jobs receives this update, it publishes a message on the `$aws/things/MyThing/jobs/notify` topic to indicate the job execution is complete:

```json
{
  "timestamp":1476290692776,
  "jobs":{}
}
```

**Additional Jobs**

If there are other job executions pending for the device, they are included in the message published to `$aws/things/MyThing/jobs/notify`.

For example:
Jobs Notifications

AWS IoT Jobs publishes MQTT messages to reserved topics when jobs are pending or when the first job execution in the list changes. Devices can keep track of pending jobs by subscribing to these topics.

Job notifications are published to MQTT topics as JSON payloads. There are two kinds of notifications:

1. **ListNotification**: A ListNotification contains a list of no more than 10 pending job executions. The job executions in this list have status values of either `IN_PROGRESS` or `QUEUED`. They are sorted by status (`IN_PROGRESS` job executions before `QUEUED` job executions) and then by the times when they were queued.

   A ListNotification is published whenever one of the following criteria is met.
   a. A new job execution is queued or changes to a non-terminal status (`IN_PROGRESS` or `QUEUED`).
   b. An old job execution changes to a terminal status (FAILED, SUCCEEDED, CANCELED, REJECTED, or REMOVED).

2. **NextNotification**: A NextNotification contains summary information about the one job execution that is next in the queue.

   A NextNotification is published whenever the first job execution in the list changes.
   a. A new job execution is added to the list as `QUEUED`, and it is the first one in the list.
   b. The status of an existing job execution that was not the first one in the list changes from `QUEUED` to `IN_PROGRESS` and becomes the first one in the list. (This happens when there are no other `IN_PROGRESS` job executions in the list or when the job execution whose status changes from `QUEUED` to `IN_PROGRESS` was queued earlier than any other `IN_PROGRESS` job execution in the list.)
   c. The status of the job execution that is first in the list changes to a terminal status and is removed from the list.

For more information about publishing and subscribing to MQTT topics, see [Message Broker for AWS IoT](p. 165)

**Note**
Notifications are not available when you use HTTP SigV4 or HTTP TLS to communicate with jobs.

AWS IoT Jobs publishes a message on an MQTT topic when a job is added to or removed from the list of pending job executions for a thing, or the first job execution in the list changes:
• $aws/things/thingName/jobs/notify
• $aws/things/thingName/jobs/notify-next

The messages contain the following example payloads:

$aws/things/thingName/jobs/notify:

```
{
  "timestamp" : 10011,
  "jobs" : {
    "IN_PROGRESS" : [ {
      "jobId" : "other-job",
      "queuedAt" : 10003,
      "lastUpdatedAt" : 10009,
      "executionNumber" : 1,
      "versionNumber" : 1
    } ],
    "QUEUED" : [ {
      "jobId" : "this-job",
      "queuedAt" : 10011,
      "lastUpdatedAt" : 10011,
      "executionNumber" : 1,
      "versionNumber" : 0
    } ]
  }
}
```

$aws/things/thingName/jobs/notify-next:

```
{
  "timestamp" : 10011,
  "execution" : {
    "jobId" : "other-job",
    "status" : "IN_PROGRESS",
    "queuedAt" : 10009,
    "lastUpdatedAt" : 10009,
    "versionNumber" : 1,
    "executionNumber" : 1,
    "jobDocument" : {"c":"d"}
  }
}
```

Possible job execution status values are QUEUED, IN_PROGRESS, FAILED, SUCCEEDED, CANCELED, REJECTED, and REMOVED.

The following series of examples shows the kinds of notifications that are published to each topic as job executions are created and change from one state to another.

First, one job, called job1, is created. This notification is published to the jobs/notify topic:

```
{
  "timestamp": 1517016948,
  "jobs": { 
    "QUEUED": [ 
      { 
        "jobId": "job1",
        "queuedAt": 1517016947,
        "lastUpdatedAt": 1517016947,
```
This notification is published to the jobs/notify-next topic:

```
{
"timestamp": 1517016948,
"execution": {
  "jobId": "job1",
  "status": "QUEUED",
  "queuedAt": 1517016947,
  "lastUpdatedAt": 1517016947,
  "versionNumber": 1,
  "executionNumber": 1,
  "jobDocument": {
    "operation": "test"
  }
}
```

When another job is created (job2), this notification is published to the jobs/notify topic:

```
{
"timestamp": 1517017192,
"jobs": {
  "QUEUED": [
    {
      "jobId": "job1",
      "queuedAt": 1517016947,
      "lastUpdatedAt": 1517016947,
      "executionNumber": 1,
      "versionNumber": 1
    },
    {
      "jobId": "job2",
      "queuedAt": 1517017191,
      "lastUpdatedAt": 1517017191,
      "executionNumber": 1,
      "versionNumber": 1
    }
  ]
}
```

A notification is not published to the jobs/notify-next topic, because the next job in the queue (job1) has not changed. When job1 starts to execute, its status changes to IN_PROGRESS. No notifications are published because the list of jobs and the next job in the queue have not changed.

When a third job (job3) is added, this notification is published to the jobs/notify topic:

```
{
"timestamp": 1517017906,
```

301
"jobs": {
    "IN_PROGRESS": [
    {
        "jobId": "job1",
        "queuedAt": 1517016947,
        "lastUpdatedAt": 1517017472,
        "startedAt": 1517017472,
        "executionNumber": 1,
        "versionNumber": 2
    }
    ],
    "QUEUED": [
    {
        "jobId": "job2",
        "queuedAt": 1517017191,
        "lastUpdatedAt": 1517017191,
        "executionNumber": 1,
        "versionNumber": 1
    },
    {
        "jobId": "job3",
        "queuedAt": 1517017905,
        "lastUpdatedAt": 1517017905,
        "executionNumber": 1,
        "versionNumber": 1
    }
    ]
}

A notification is not published to the jobs/notify-next topic because the next job in the queue is still job1.

When job1 is complete, its status changes to SUCCEEDED, and this notification is published to the jobs/notify topic:

{ "timestamp": 1517186269,
  "jobs": { "QUEUED": [ { "jobId": "job2",
                            "queuedAt": 1517017191,
                            "lastUpdatedAt": 1517017191,
                            "executionNumber": 1,
                            "versionNumber": 1
                            },
                            { "jobId": "job3",
                            "queuedAt": 1517017905,
                            "lastUpdatedAt": 1517017905,
                            "executionNumber": 1,
                            "versionNumber": 1
                            }
                        ]
  }
}

At this point, job1 has been removed from the queue, and the next job to be executed is job2. This notification is published to the jobs/notify-next topic:
If job3 needs to begin executing before job2 (which is not recommended), the status of job3 can be changed to IN_PROGRESS. If this happens, job2 is no longer next in the queue, and this notification is published to the jobs/notify-next topic:

```json
{
"timestamp": 1517186779,
"execution": {
   "jobId": "job3",
   "status": "IN_PROGRESS",
   "queuedAt": 1517017905,
   "startedAt": 1517186779,
   "lastUpdatedAt": 1517186779,
   "versionNumber": 2,
   "executionNumber": 1,
   "jobDocument": {
      "operation": "test"
   }
}
}
```

No notification is published to the jobs/notify topic because no job has been added or removed.

If the device rejects job2 and updates its status to REJECTED, this notification is published to the jobs/notify topic:

```json
{
"timestamp": 1517189392,
"jobs": {
   "IN_PROGRESS": [
      {
         "jobId": "job3",
         "queuedAt": 1517017905,
         "lastUpdatedAt": 1517186779,
         "startedAt": 1517186779,
         "executionNumber": 1,
         "versionNumber": 2
      }
   ]
}
```
If job3 (which is still in progress) is force deleted, this notification is published to the `jobs/notify` topic:

```json
{
    "timestamp": 1517189551,
    "jobs": {}
}
```

At this point, the queue is empty. This notification is published to the `jobs/notify-next` topic:

```json
{
    "timestamp": 1517189551
}
```

## Using the AWS IoT Jobs APIs

There are two categories of API used in AWS IoT Jobs:

- Those used for management and control of jobs.
- Those used by the devices executing those jobs.

In general, job management and control uses an HTTPS protocol API. Devices can use either an MQTT or an HTTPS protocol API. (The HTTPS API is designed for a low volume of calls typical when creating and tracking jobs. It usually opens a connection for a single request, and then closes the connection after the response is received. The MQTT API allows long polling. It is designed for large amounts of traffic that can scale to millions of devices.)

**Note**

Each Jobs HTTPS API has a corresponding command that allows you to call the API from the AWS CLI. The commands are lowercase, with hyphens between the words that make up the name of the API. For example, you can invoke the CreateJob API on the CLI by typing:

```
aws iot create-job ...
```

## Job Management and Control API

### Job Management and Control Data Types

The following data types are used by management and control applications to communicate with Jobs.

**Job**

Job data type

The Job object contains details about a job.

**syntax (1)**

```json
{
    "jobArn": "string",
    "jobId": "string",
```
"status": "IN_PROGRESS|CANCELED|COMPLETED",
"forceCanceled": boolean,
"targetSelection": "CONTINUOUS|SNAPSHOT",
"comment": "string",
"targets": ["string"],
"description": "string",
"createdAt": timestamp,
"lastUpdatedAt": timestamp,
"completedAt": timestamp,
"jobProcessDetails": {
  "processingTargets": ["string"],
  "numberOfCanceledThings": "long",
  "numberOfSucceededThings": "long",
  "numberOfFailedThings": "long",
  "numberOfRejectedThings": "long",
  "numberOfQueuedThings": "long",
  "numberOfInProgressThings": "long",
  "numberOfRemovedThings": "long",
},
"presignedUrlConfig": {
  "expiresInSec": number,
  "roleArn": "string"
},
"jobExecutionRolloutConfig": {
  "maximumPerMinute": "integer"
}

description (1)

jobArn

An ARN identifying the job with the format "arn:aws:iot:region:account:job/jobId".

jobId

The unique identifier you assigned to this job when it was created.

status

The status of the job, one of IN_PROGRESS, CANCELED, or COMPLETED.

targetSelection

Specifies whether the job continues to run (CONTINUOUS) or is complete after those things specified as targets have completed the job (SNAPSHOT). If CONTINUOUS, the job might also be run on a thing when a change is detected in a target. For example, a job runs on a thing when the thing is added to a target group, even after the job was completed by all things originally in the group.

comment

If the job was updated, describes the reason for the update.

targets

A list of AWS IoT things and thing groups to which the job should be sent.

description

A short text description of the job.

createdAt

The time, in milliseconds since the epoch, when the job was created.

lastUpdatedAt

The time, in milliseconds since the epoch, when the job was last updated.
completedAt

The time, in milliseconds since the epoch, when the job was completed.

jobProcessDetails

Details about the job process:

processingTargets

A list of AWS IoT things and thing groups that are currently executing the job.

numberOfCanceledThings

The number of AWS IoT things that canceled the job.

numberOfSucceededThings

The number of AWS IoT things that successfully completed the job.

numberOfFailedThings

The number of AWS IoT things that failed to complete the job.

numberOfRejectedThings

The number of AWS IoT things that rejected the job.

numberOfQueuedThings

The number of AWS IoT things that are awaiting execution of the job.

numberOfInProgressThings

The number of AWS IoT things that are currently executing the job.

numberOfRemovedThings

The number of AWS IoT things that are no longer scheduled to execute the job because they have been deleted or removed from the group that was a target of the job.

presignedUrlConfig

Configuration information for presigned Amazon S3 URLs.

expiresInSec

How long (in seconds) presigned URLs are valid. Valid values are 60 - 3600. The default value is 3600 seconds. Presigned URLs are generated when Jobs receives an MQTT request for the job document.

roleArn

The ARN of an IAM role that grants permission to download files from an Amazon S3 bucket. The role must also grant permission for AWS IoT to download the files. For more information about how to create and configure the role, see Create Jobs (p. 282).

jobExecutionRolloutConfig

Allows you to create a staged rollout of a job.

maximumPerMinute

The maximum number of things (devices) to which the job will be sent for execution, per minute.

JobSummary

JobSummary data type

The JobSummary object contains a job summary.
syntax (2)

```
{
    "jobArn": "string",
    "jobId": "string",
    "status": "IN_PROGRESS|CANCELED|COMPLETED",
    "targetSelection": "CONTINUOUS|SNAPSHOT",
    "thingGroupId": "string",
    "createdAt": timestamp,
    "lastUpdatedAt": timestamp,
    "completedAt": timestamp
}
```

description (2)

**jobArn**

An ARN that identifies the job.

**jobId**

The unique identifier you assigned to this job when it was created.

**status**

The job status. Can be one of IN_PROGRESS, CANCELED, or COMPLETED.

**targetSelection**

Specifies whether the job continues to run (CONTINUOUS) or is complete after all those things specified as targets have completed the job (SNAPSHOT). If CONTINUOUS, the job might also be run on a thing when a change is detected in a target. For example, a job runs on a thing when the thing is added to a target group, even after the job was completed by all things originally in the group.

**thingGroupId**

The ID of the thing group.

**createdAt**

The UNIX timestamp for when the job was created.

**lastUpdatedAt**

The UNIX timestamp for when the job was last updated.

**completedAt**

The UNIX timestamp for when the job was completed.

**JobExecution**

**JobExection data type**

The JobExecution object represents the execution of a job on a particular device.

syntax (3)

```
{
    "executionNumber": 1234567890,
    "forceCanceled": true|false,
    "jobId": "string",
    "lastUpdatedAt": timestamp,
```
"queuedAt": timestamp,
"startedAt": timestamp,
"status": "QUEUED|IN_PROGRESS|FAILED|SUCCESS|CANCELED|REJECTED|REMOVED",
"forceCanceled": boolean,
"statusDetails": {
    "detailsMap": {
        "string": "string" ...
    },
    "status": "string"
},
"thingArn": "string",
"versionNumber": 123

description (3)

jobId

The unique identifier you assigned to this job when it was created.

executionNumber

A number that identifies this job execution on this particular device. It can be used later in commands that return or update job execution information.

thingArn

The AWS IoT thing ARN.

queuedAt

The time, in milliseconds since the epoch, when the job execution was queued.

lastUpdatedAt

The time, in milliseconds since the epoch, when the job execution was last updated.

startedAt

The time, in milliseconds since the epoch, when the job execution was started.

status

The status of the job execution. Can be one of "QUEUED", "IN_PROGRESS", "FAILED", "SUCCESS", "CANCELED", "REJECTED", or "REMOVED".

statusDetails

A collection of name/value pairs that describe the status of the job execution.

JobExecutionSummary

JobExecutionSummary data type

The JobExecutionSummary object contains job execution summary information:

syntax (4)

```
{"executionNumber": 1234567890,
"queuedAt": timestamp,
"lastUpdatedAt": timestamp,
"startedAt": timestamp,
"status": "QUEUED|IN_PROGRESS|FAILED|SUCCESS|CANCELED|REJECTED|REMOVED"
}
```
description (4)

executionNumber

A number that identifies a particular job execution on a particular device. It can be used later in commands that return or update job execution information.

queuedAt

The time, in milliseconds since the epoch, when the job execution was queued.

lastUpdatedAt

The time, in milliseconds since the epoch, when the job execution was last updated.

startAt

The time, in milliseconds since the epoch, when the job execution was started.

status

The status of the job execution: QUEUED, IN_PROGRESS, FAILED, SUCCESS, CANCELED, REJECTED, or REMOVED.

JobExecutionSummaryForJob

JobExecutionSummaryForJob data type

The JobExecutionSummaryForJob object contains a summary of information about job executions for a specific job.

syntax (5)

```json
{
  "executionSummary": [
    {
      "thingArn": "string",
      "jobExecutionSummary": { JobExecutionSummary }
    }
    ...
  ]
}
```

description (5)

thingArn

The AWS IoT thing ARN.

jobExecutionSummary

An JobExecutionSummary (p. 308) object.

JobExecutionSummaryForThing

JobExecutionSummaryForThing data type

The JobExecutionSummaryForThing object contains a summary of information about a job execution on a specific thing.

syntax (6)

```json
{
```

309
"jobId": "string",
"jobExecutionSummary": { JobExecutionSummary }
}

description (6)

jobId

The unique identifier you assigned to this job when it was created.

jobExecutionSummary

A JobExecutionSummary (p. 308) object.

Job Management and Control HTTPS Commands

The following commands are available for management and control applications over the HTTPS protocol.

AssociateTargetsWithJob

AssociateTargetsWithJob command

Associates a group with a continuous job. For more information, see CreateJob (p. 317). The following criteria must be met:

- The job must have been created with the targetSelection field set to "CONTINUOUS".
- The job status must currently be "IN_PROGRESS".
- The total number of targets associated with a job must not exceed 100.

HTTPS (1)

Request:

POST /jobs/jobId/targets

{
   "targets": [ "string" ],
   "comment": "string"
}

jobId

The unique identifier you assigned to this job when it was created.

targets

A list of thing group ARNs that define the targets of the job.

comment

Optional. A comment string that describes why the job was associated with the targets.

Response:

{
   "jobArn": "string",
   "jobId": "string",
   "description": "string"
jobArn

An ARN identifying the job.

jobId

The unique identifier you assigned to this job when it was created.

description

A short text description of the job.

CLI (1)

Synopsis:

```
aws iot  associate-targets-with-job \n   --targets <value> \n   --job-id <value> \n   [--comment <value>] \n   [--cli-input-json <value>] \n   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "targets": [
      "string"
   ],
   "jobId": "string",
   "comment": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targets</td>
<td>list</td>
<td>A list of thing group ARNs that define the targets of the job.</td>
</tr>
<tr>
<td></td>
<td>member: TargetArn</td>
<td></td>
</tr>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>length max:64 min:1</td>
<td>pattern: [a-zA-Z0-9-_]+</td>
</tr>
<tr>
<td>comment</td>
<td>string</td>
<td>An optional comment string describing why the job was associated with the targets.</td>
</tr>
<tr>
<td></td>
<td>length max:2028</td>
<td>pattern: [^\p{C}]+</td>
</tr>
</tbody>
</table>

Output:

```
{
```

311
"jobArn": "string",
"jobId": "string",
"description": "string"
}

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobArn</td>
<td>string</td>
<td>An ARN identifying the job.</td>
</tr>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>A short text description of the job.</td>
</tr>
</tbody>
</table>

MQTT (1)

Not available.

**CancelJob**

CancelJob command

Cancels a job.

**HTTPS (2)**

Request:

```
PUT /jobs/jobId/cancel
{
    "force": "boolean",
    "comment": "string"
}
```

jobId

The unique identifier you assigned to this job when it was created.

force

[Optional] If true job executions with status "IN_PROGRESS" and "QUEUED" are canceled, otherwise only job executions with status "QUEUED" are canceled. The default is false.

**Warning**

Canceling a job which is "IN_PROGRESS", will cause a device which is executing the job to be unable to update the job execution status. Use caution and ensure that each device executing a job which is canceled is able to recover to a valid state.

comment

[Optional] A comment string describing why the job was canceled.
Response:

```
{
  "jobArn": "string",
  "jobId": "string",
  "description": "string"
}
```

**jobArn**

The job ARN.

**jobId**

The unique identifier you assigned to this job when it was created.

**description**

A short text description of the job.

**CLI (2)**

**Synopsis:**

```
aws iot cancel-job \
  --job-id <value> \
  [--force <value>] \
  [--comment <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

**cli-input-json format:**

```
{
  "jobId": "string",
  "force": "boolean",
  "comment": "string"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>length max:64 min:1 pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>force</td>
<td>boolean</td>
<td>If true, jobs with status QUEUED and IN_PROGRESS will be canceled, otherwise only jobs with status QUEUED will be canceled.</td>
</tr>
</tbody>
</table>

**Warning**

Canceling a job which is "IN_PROGRESS", will cause a device which is executing the job to
Name | Type | Description
--- | --- | ---
be unable to update the job execution status. Use caution and ensure that each device executing a job which is canceled is able to recover to a valid state.

comment | string | An optional comment string describing why the job was canceled.

length max:2028
pattern: [^\\p{C}]+

Output:

```json
{
    "jobArn": "string",
    "jobId": "string",
    "description": "string"
}
```

cli output fields:

Name | Type | Description
--- | --- | ---
jobArn | string | The job ARN.
jobId | string | The unique identifier you assigned to this job when it was created.

length max:64 min:1
pattern: [a-zA-Z0-9-]+
description | string | A short text description of the job.

length max:2028
pattern: [^\\p{C}]+

MQTT (2)

Not available.

**CancelJobExecution**

CancelJobExecution command

Cancels a job execution on a particular device.

HTTPS (3)

Request:

```
PUT /things/thingName/jobs/jobId/cancel
```
thingName

The name of the thing whose job execution will be canceled.

jobId

The unique identifier you assigned to the job when it was created.

force

Optional. If true a job execution with status "IN_PROGRESS" or "QUEUED" can be canceled, otherwise only a job execution with status "QUEUED" can be canceled. If you attempt to cancel a job execution that is "IN_PROGRESS" and you do not set force to true, then an InvalidStateTransitionException will be thrown. The default is false.

Warning

Canceling a job which is "IN_PROGRESS", will cause a device which is executing the job to be unable to update the job execution status. Use caution and ensure that each device executing a job which is cancelled is able to recover to a valid state.

expectedVersion

Optional. The expected current version of the job execution. Each time you update the job execution, its version is incremented. If the version of the job execution stored in Jobs does not match, the update is rejected with a VersionConflictException error, and an ErrorResponse that contains the current job execution status data is returned. (This makes it unnecessary to perform a separate DescribeJobExecution request in order to obtain the job execution status data.)

statusDetails

Optional. A collection of name/value pairs that describe the status of the job execution.

Response:

{
}

CLI (3)

Synopsis:

aws iot cancel-job-execution
  --job-id <value> \
  --thing-name <value> \n  [--force | --no-force] \n  [--expected-version <value>] \n  [--status-details <value>] \n  [--cli-input-json <value>] \n  [--generate-cli-skeleton]

cli-input-json format:

{
}
"jobId": "string",
"thingName": "string",
"force": "boolean",
"expectedVersion": "long",
"statusDetails": {
    "string": "string"
}
}

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The job to be canceled.</td>
</tr>
<tr>
<td></td>
<td>length max:64 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9_]+</td>
<td></td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing whose execution of the job will be canceled.</td>
</tr>
<tr>
<td></td>
<td>length max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]</td>
<td></td>
</tr>
<tr>
<td>force</td>
<td>boolean</td>
<td>Optional. If true the job execution will be canceled if it has status IN_PROGRESS or QUEUED, otherwise the job execution will be canceled only if it has status QUEUED. However, if you attempt to cancel a job execution that is IN_PROGRESS, and you do not set --force to true, then an InvalidStateTransitionException will be thrown. The default is false.</td>
</tr>
<tr>
<td>expectedVersion</td>
<td>long</td>
<td>Optional. The expected current version of the job execution. Each time you update the job execution, its version is increment. If the version of the job execution stored in Jobs does not match,</td>
</tr>
<tr>
<td></td>
<td>java class: java.lang.Long</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the update is rejected with a VersionMismatch error, and an ErrorResponse that contains the current job execution status data is returned. (This makes it unnecessary to perform a separate DescribeJobExecution request in order to obtain the job execution status data.)</td>
</tr>
<tr>
<td>statusDetails</td>
<td>map</td>
<td>A collection of name/value pairs that describe the status of the job execution. If not specified, the statusDetails are unchanged.</td>
</tr>
<tr>
<td>DetailsKey</td>
<td>string</td>
<td>length max:128 min:1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pattern: [a-zA-Z0-9-_:]+</td>
</tr>
<tr>
<td>DetailsValue</td>
<td>string</td>
<td>length max:1024 min:1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pattern: [^\p{C}]*+</td>
</tr>
</tbody>
</table>

Output:
None
MQTT (3)
Not available.

**CreateJob**

CreateJob command

Create a job. You can provide the job document as a link to a file in an Amazon S3 bucket (documentSource parameter) or in the body of the request (document parameter).

A job can be made continuous by setting the optional targetSelection parameter to "CONTINUOUS". (The default is "SNAPSHOT".) A continuous job can be used to onboard or upgrade devices as they are added to a group because it continues to run and is executed on newly added things, even after the things in the group at the time the job was created have completed the job.

The following validations are performed on arguments to the CreateJob API:

- The targets argument must be a list of valid thing or thing group ARNs. All things and thing groups must be in your AWS account.
- The documentSource argument must be a valid Amazon S3 URL to a job document. Amazon S3 URLs are of the form: https://s3.amazonaws.com/bucketName/objectName.
- The document stored in the URL specified by the documentSource argument must be a UTF-8 encoded JSON document.
The size of a job document is limited to 32 KB due to the limit on the size of an MQTT message (128 KB) and encryption.

The jobId must be unique within your AWS account.

### HTTPS (4)

**Request:**

```plaintext
PUT /jobs/jobId
{
  "targets": [ "string" ],
  "document": "string",
  "documentSource": "string",
  "description": "string",
  "presignedUrlConfigData": {
    "roleArn": "string",
    "expiresInSec": "integer"
  },
  "targetSelection": "CONTINUOUS|SNAPSHOT",
  "jobExecutionsRolloutConfig": {
    "maximumPerMinute": "integer"
  }
}
```

**jobId**

A job identifier, which must be unique for your AWS account. We recommend using a UUID. Alpha-numeric characters, ",", and ",_" can be used here.

**targets**

A list of thing or thing group ARNs that defines the targets of the job.

**document**

Optional. The job document.

**documentSource**

Optional. An Amazon S3 link to the job document.

**description**


**presignedUrlConfigData**

Optional. Configuration information for presigned Amazon S3 URLs.

**roleArn**

The ARN of the IAM role that contains permissions to access the Amazon S3 bucket. This is the bucket that contains the data that devices download with the presigned Amazon S3 URLs. This role must also grant AWS IoT permission to assume the role. For more information, see Create Jobs (p. 282).

**expiresInSec**

How long (in seconds) presigned URLs are valid. Valid values are 60 - 3600. The default value is 3600 seconds. Presigned URLs are generated when Jobs receives an MQTT request for the job document.

**targetSelection**

Optional. Specifies whether the job continues to run (CONTINUOUS) or is complete after all those things specified as targets have completed the job (SNAPSHOT). If CONTINUOUS, the job...
might also be scheduled to run on a thing when a change is detected in a target. For example, a
job is scheduled to run on a thing when the thing is added to a target group, even after the job
was completed by all things originally in the group.

**jobExecutionRolloutConfig**

Optional. Allows you to create a staged rollout of a job.

**maximumPerMinute**

The maximum number of things on which the job is sent for execution, per minute. Valid
values are 1 to 1000. If not specified, the default is 1000. The actual number of things that
receive the job might be less during any particular minute interval (due to system latency),
but will not be more than the specified value.

Response:

```json
{
    "jobArn": "string",
    "jobId": "string",
    "description": "string"
}
```

**jobArn**

The ARN of the job.

**jobId**

The unique identifier you assigned to this job.

**description**

An optional short text description of the job.

**CLI (4)**

**Synopsis:**

```
aws iot  create-job \
   --job-id <value> \
   --targets <value> \
       [--document-source <value>] \
       [--document <value>] \
       [--description <value>] \
       [--presigned-url-config <value>] \
       [--target-selection <value>] \
       [--job-executions-rollout-config <value>] \
       [--document-parameters <value>] \
       [--cli-input-json <value>] \
       [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
    "jobId": "string",
    "targets": [
        "string"
    ],
    "documentSource": "string",
    "document": "string",
    "description": "string",
```
"presignedUrlsConfig": {
  "roleArn": "string",
  "expiresInSec": "long"
},
"targetSelection": "string",
"jobExecutionsRolloutConfig": {
  "maximumPerMinute": "integer"
},
"documentParameters": {
  "string": "string"
}

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>A job identifier which must be unique for your AWS account. We recommend using a UUID. Alpha-numeric characters, &quot;.&quot; and &quot;_&quot; are valid for use here.</td>
</tr>
<tr>
<td>targets</td>
<td>list</td>
<td>A list of things and thing groups to which the job should be sent.</td>
</tr>
<tr>
<td>TargetArn</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>documentSource</td>
<td>string</td>
<td>An S3 link to the job document.</td>
</tr>
<tr>
<td>document</td>
<td>string</td>
<td>The job document.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>A short text description of the job.</td>
</tr>
<tr>
<td>presignedUrlsConfig</td>
<td>PresignedUrlConfig</td>
<td>Configuration information for pre-signed S3 URLs.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of an IAM role that grants permission to download files from the S3 bucket where the job data/updates are stored. The role must also grant permission for IoT to download the files.</td>
</tr>
<tr>
<td>expiresInSec</td>
<td>long</td>
<td>How long (in seconds) pre-signed URLs are valid. Valid values are 60 - 3600, the default value is 3600 seconds. Pre-signed URLs are generated when Jobs receives an MQTT request for the job document.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>targetSelection</td>
<td>string enum: CONTINUOUS</td>
<td>Specifies whether the job will continue to run (CONTINUOUS), or will be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>complete after all those things specified as targets have completed the job</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(SNAPSHOT). If continuous, the job may also be run on a thing when a change</td>
</tr>
<tr>
<td></td>
<td></td>
<td>is detected in a target. For example, a job will run on a thing when the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>thing is added to a target group, even after the job was completed by all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>things originally in the group.</td>
</tr>
<tr>
<td>jobExecutionsRolloutConfig</td>
<td>JobExecutionsRolloutConfig</td>
<td>Allows you to create a staged rollout of the job.</td>
</tr>
<tr>
<td>maximumPerMinute</td>
<td>integer java class:</td>
<td>The maximum number of things that will be notified of a pending job, per</td>
</tr>
<tr>
<td></td>
<td>java.lang.Integer</td>
<td>minute. This parameter allows you to create a staged rollout.</td>
</tr>
<tr>
<td>documentParameters</td>
<td>map key: ParameterKey</td>
<td>Parameters for the job document.</td>
</tr>
<tr>
<td>ParameterKey</td>
<td>string length max:128</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>ParameterValue</td>
<td>string length max:1024</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [^\p{C}]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
    "jobArn": "string",
    "jobId": "string",
    "description": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobArn</td>
<td>string</td>
<td>The job ARN.</td>
</tr>
</tbody>
</table>
### Job Management and Control API

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job.</td>
</tr>
<tr>
<td>length</td>
<td>max:64 min:1</td>
<td></td>
</tr>
<tr>
<td>pattern</td>
<td>[a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>The job description.</td>
</tr>
<tr>
<td>length</td>
<td>max:2028</td>
<td></td>
</tr>
<tr>
<td>pattern</td>
<td>[^\p{C}]++</td>
<td></td>
</tr>
</tbody>
</table>

**MQTT (4)**

Not available.

**DeleteJob**

DeleteJob command

Deletes a job and its related job executions.

Deleting a job may take time, depending on the number of job executions created for the job and various other factors. While the job is being deleted, the status of the job will be shown as "DELETION_IN_PROGRESS". Attempting to delete or cancel a job whose status is already "DELETION_IN_PROGRESS" will result in an error.

**HTTPS (4)**

**Request syntax:**

```
DELETE /jobs/jobId?force=force
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>JobId</td>
<td>yes</td>
<td>The ID of the job to be deleted.</td>
</tr>
<tr>
<td>force</td>
<td>ForceFlag</td>
<td>no</td>
<td>(Optional) When true, you can delete a job which is &quot;IN_PROGRESS&quot;. Otherwise, you can only delete a job which is in a terminal state (&quot;COMPLETED&quot; or &quot;CANCELED&quot;) or an exception will occur. The default is false.</td>
</tr>
</tbody>
</table>

**Note**

Deleting a job which is "IN_PROGRESS",
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>will cause a device which</td>
<td></td>
<td></td>
<td>device which is executing the job to be unable to access job information or update the job execution status. Use caution and ensure that each device executing a job which is deleted is able to recover to a valid state.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**InvalidStateTransitionException**

An update attempted to change the job or job execution to a state that is invalid because of its current state (for example, an attempt to change a request in state SUCCESS to state IN_PROGRESS). In this case, the body of the error message also contains the executionState field.

HTTP response code: 409

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**ServiceUnavailableException**

The service is temporarily unavailable.

HTTP response code: 503

**Synopsis:**
aws iot delete-job
   --job-id <value>
   [--force | --no-force] 
   [--cli-input-json <value>] 
   [--generate-cli-skeleton]

cli-input-json format:

{
   "jobId": "string",
   "force": "boolean"
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobld</td>
<td>string</td>
<td>The ID of the job to be deleted. The ID of the job to be deleted.</td>
</tr>
<tr>
<td></td>
<td>length</td>
<td>max:64 min:1 length max:64 min:1</td>
</tr>
<tr>
<td></td>
<td>pattern</td>
<td>[a-zA-Z0-9-_]+</td>
</tr>
<tr>
<td>force</td>
<td>boolean</td>
<td>(Optional) When true, you can delete a job which is &quot;IN_PROGRESS&quot;. Otherwise, you can only delete a job which is in a terminal state (&quot;COMPLETED&quot; or &quot;CANCELED&quot;) or an exception will occur. The default is false.</td>
</tr>
</tbody>
</table>

Note
Deleting a job which is "IN_PROGRESS", will cause a device which is executing the job to be unable to access job information or update the job execution status. Use caution and ensure that each device executing a job which is deleted is able to recover to a valid state.

Output:
None
MQTT (4)
Not available.
DeleteJobExecution

DeleteJobExecution command

Deletes a job execution.

HTTPS (5)

Request syntax:

```
DELETE /things/thingName/jobs/jobId/executionsNumber/executionNumber?force=force
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>JobId</td>
<td>yes</td>
<td>The ID of the job whose execution will be deleted.</td>
</tr>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing whose execution of the job will be deleted.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>ExecutionNumber</td>
<td>yes</td>
<td>The ID of the job execution to be deleted.</td>
</tr>
<tr>
<td>force</td>
<td>ForceFlag</td>
<td>no</td>
<td>When true, you can delete a job execution which is &quot;IN_PROGRESS&quot;. Otherwise, you can only delete a job execution which is in a terminal state (&quot;SUCCEEDED&quot;, &quot;FAILED&quot;, &quot;REJECTED&quot;, &quot;REMOVED&quot; or &quot;CANCELED&quot;) or an exception will occur. The default is false.</td>
</tr>
</tbody>
</table>

**Note**
Deleting a job execution which is "IN_PROGRESS" will cause the device to be unable to access job information or update the job execution status. Use caution and ensure that the device
is able to recover to a valid state.

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**InvalidStateTransitionException**

An update attempted to change the job execution to a state that is invalid because of the job execution's current state (for example, an attempt to change a request in state SUCCESS to state IN_PROGRESS). In this case, the body of the error message also contains the executionState field.

HTTP response code: 409

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**ServiceUnavailableException**

The service is temporarily unavailable.

HTTP response code: 503

**CLI (5)**

**Synopsis:**

```bash
aws iot delete-job-execution \   --job-id <value> \   --thing-name <value> \   --execution-number <value> \   [--force | --no-force] \   [--cli-input-json <value>] \   [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
    "jobId": "string",
    "thingName": "string",
    "executionNumber": "long",
    "force": "boolean"
}
```
cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The ID of the job whose execution will be deleted.</td>
</tr>
<tr>
<td></td>
<td>length max:64 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing whose execution of the job will be deleted.</td>
</tr>
<tr>
<td></td>
<td>length max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_:]+</td>
<td></td>
</tr>
<tr>
<td>executionNumber</td>
<td>long</td>
<td>The ID of the job execution to be deleted.</td>
</tr>
<tr>
<td></td>
<td>java class: java.lang.Long</td>
<td></td>
</tr>
<tr>
<td>force</td>
<td>boolean</td>
<td>When true, you can delete a job execution which is &quot;IN_PROGRESS&quot;. Otherwise,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>you can only delete a job execution which is in a terminal state (&quot;SUCCEEDED&quot;, &quot;FAILED&quot;, &quot;REJECTED&quot;, &quot;REMOVED&quot; or &quot;CANCELED&quot;) or an exception will occur. The default is false.</td>
</tr>
</tbody>
</table>

Note
Deleting a job execution which is "IN_PROGRESS" will cause the device to be unable to access job information or update the job execution status. Use caution and ensure that the device is able to recover to a valid state.

Output:
None
MQTT (5)
Not available.

DescribeJob

DescribeJob command

Gets the details of the specified job.
HTTPS (6)

Request:

GET /jobs/jobId

jobId

The unique identifier you assigned to this job when it was created.

Response:

{  
  "documentSource": "string",
  "job": Job
}

documentSource

An Amazon S3 link to the job document.

job

A Job (p. 304) object.

CLI (6)

Synopsis:

aws iot describe-job \
  --job-id <value>  \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]

cli-input-json format:

{
  "jobId": "string"
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>length max:64 min:1 pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

{  
  "documentSource": "string",
  "job": {
    "jobArn": "string",
    "jobId": "string",
    "targetSelection": "string",
  }
}
"status": "string",
"forceCanceled": "boolean",
"comment": "string",
"targets": [
  "string"
],
"description": "string",
"presignedUrlConfig": {
  "roleArn": "string",
  "expiresInSec": "long"
},
"jobExecutionsRolloutConfig": {
  "maximumPerMinute": "integer"
},
"createdAt": "timestamp",
"lastUpdatedAt": "timestamp",
"completedAt": "timestamp",
"jobProcessDetails": {
  "processingTargets": [
    "string"
  ],
  "numberOfCanceledThings": "integer",
  "numberOfSucceededThings": "integer",
  "numberOfFailedThings": "integer",
  "numberOfRejectedThings": "integer",
  "numberOfQueuedThings": "integer",
  "numberOfInProgressThings": "integer",
  "numberOfRemovedThings": "integer"
},
"documentParameters": {
  "string": "string"
}
}

### cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>documentSource</td>
<td>string</td>
<td>An S3 link to the job document.</td>
</tr>
<tr>
<td></td>
<td>length max:1350 min:1</td>
<td></td>
</tr>
<tr>
<td>job</td>
<td>Job</td>
<td>Information about the job.</td>
</tr>
<tr>
<td>jobArn</td>
<td>string</td>
<td>An ARN identifying the job with format &quot;arn:aws:iot:region:account:job/jobId&quot;.</td>
</tr>
<tr>
<td>jobld</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>length max:64 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>targetSelection</td>
<td>string</td>
<td>Specifies whether the job will continue to run (CONTINUOUS), or will be complete after all those things specified as targets have completed the job (SNAPSHOT). If continuous, the</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>job may also be run on a thing when a change is detected in a target. For example, a job will run on a device when the thing representing the device is added to a target group, even after the job was completed by all things originally in the group.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the job, one of IN_PROGRESS, CANCELED, or COMPLETED.</td>
</tr>
<tr>
<td>forceCanceled</td>
<td>boolean</td>
<td>Will be true if the job was canceled with the optional force parameter set to true.</td>
</tr>
<tr>
<td>comment</td>
<td>string</td>
<td>If the job was updated, describes the reason for the update.</td>
</tr>
<tr>
<td>targets</td>
<td>list</td>
<td>A list of IoT things and thing groups to which the job should be sent.</td>
</tr>
<tr>
<td>TargetArn</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>A short text description of the job.</td>
</tr>
<tr>
<td>presignedUrlConfig</td>
<td>PresignedUrlConfig</td>
<td>Configuration for pre-signed S3 URLs.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of an IAM role that grants permission to download files from the S3 bucket where the job data/updates are stored. The role must also grant permission for IoT to download the files.</td>
</tr>
<tr>
<td>expiresInSec</td>
<td>long</td>
<td>How long (in seconds) pre-signed URLs are valid. Valid values are 60 - 3600, the default value is 3600 seconds. Pre-signed URLs are generated when Jobs receives an MQTT request for the job document.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>jobExecutionsRolloutConfig</td>
<td>JobExecutionsRolloutConfig</td>
<td>Allows you to create a staged rollout of a job.</td>
</tr>
<tr>
<td>maximumPerMinute</td>
<td>integer</td>
<td>The maximum number of things that will be notified of a pending job, per minute. This parameter allows you to create a staged rollout.</td>
</tr>
<tr>
<td></td>
<td>java class: java.lang.Integer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>range- max:1000 min:1</td>
<td></td>
</tr>
<tr>
<td>createdAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job was created.</td>
</tr>
<tr>
<td>lastUpdatedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job was last updated.</td>
</tr>
<tr>
<td>completedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job was completed.</td>
</tr>
<tr>
<td>jobProcessDetails</td>
<td>JobProcessDetails</td>
<td>Details about the job process.</td>
</tr>
<tr>
<td>processingTargets</td>
<td>list</td>
<td>The devices on which the job is executing.</td>
</tr>
<tr>
<td></td>
<td>member: ProcessingTargetName</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>ProcessingTargetName</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>numberOfCanceledThings</td>
<td>integer</td>
<td>The number of things that cancelled the job.</td>
</tr>
<tr>
<td></td>
<td>java class: java.lang.Integer</td>
<td></td>
</tr>
<tr>
<td>numberOfSucceededThings</td>
<td>integer</td>
<td>The number of things which successfully completed the job.</td>
</tr>
<tr>
<td></td>
<td>java class: java.lang.Integer</td>
<td></td>
</tr>
<tr>
<td>numberOfFailedThings</td>
<td>integer</td>
<td>The number of things that failed executing the job.</td>
</tr>
<tr>
<td></td>
<td>java class: java.lang.Integer</td>
<td></td>
</tr>
<tr>
<td>numberOfRejectedThings</td>
<td>integer</td>
<td>The number of things that rejected the job.</td>
</tr>
<tr>
<td></td>
<td>java class: java.lang.Integer</td>
<td></td>
</tr>
<tr>
<td>numberOfQueuedThings</td>
<td>integer</td>
<td>The number of things that are awaiting execution of the job.</td>
</tr>
<tr>
<td></td>
<td>java class: java.lang.Integer</td>
<td></td>
</tr>
<tr>
<td>numberOfInProgressThings</td>
<td>integer</td>
<td>The number of things currently executing the job.</td>
</tr>
<tr>
<td></td>
<td>java class: java.lang.Integer</td>
<td></td>
</tr>
</tbody>
</table>
### Name | Type | Description
--- | --- | ---
numberOfRemovedThings | integer | The number of things that are no longer scheduled to execute the job because they have been deleted or have been removed from the group that was a target of the job.

documentParameters | map | The parameters specified for the job document.

**ParameterKey**
- string
- length max:128 min:1
- pattern: [a-zA-Z0-9-_]+

**ParameterValue**
- string
- length max:1024 min:1
- pattern: [^\p{C}]+

MQTT (6)
Not available.

**DescribeJobExecution**

DescribeJobExecution command

Gets details of a job execution. The job's execution status must be SUCCEEDED or FAILED.

HTTPS (7)

**Request:**

```
GET /things/thingName/jobs/jobId?executionNumber=executionNumber
```

**jobId**

The unique identifier you assigned to this job when it was created.

**thingName**

The thing name associated with the device the job execution is running on.

**executionNumber**

Optional. A number that is used to specify a particular job execution on a particular device. (See JobExecution (p. 307).) If not specified, the latest job execution is returned.

**Response:**

```json
{
  "execution": { JobExecution }
}
```
A JobExecution (p. 307) object.

CLI (7)

Synopsis:

```bash
aws iot describe-job-execution
   --job-id <value> \
   --thing-name <value> \
   [--execution-number <value>] \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
   "jobId": "string",
   "thingName": "string",
   "executionNumber": "long"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>length max:64 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing on which the job execution is running.</td>
</tr>
<tr>
<td></td>
<td>length max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>executionNumber</td>
<td>long</td>
<td>A string (consisting of the digits &quot;0&quot; through &quot;9&quot; which is used to specify a particular job execution on a particular device.</td>
</tr>
</tbody>
</table>

Output:

```json
{
   "execution": {
      "jobId": "string",
      "status": "string",
      "forceCanceled": "boolean",
      "statusDetails": {
         "detailsMap": {
            "string": "string"
         }
      }
   }
}
```
"thingArn": "string",
"queuedAt": "timestamp",
"startedAt": "timestamp",
"lastUpdatedAt": "timestamp",
"executionNumber": "long",
"versionNumber": "long"
}
}

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>execution</td>
<td>JobExecution</td>
<td>Information about the job execution.</td>
</tr>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to the job when it was created.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the job execution (IN_PROGRESS, QUEUED, FAILED, SUCCESS, CANCELED, or REJECTED).</td>
</tr>
<tr>
<td>forceCanceled</td>
<td>boolean</td>
<td>Will be true if the job execution was canceled with the optional force parameter set to true.</td>
</tr>
<tr>
<td>statusDetails</td>
<td>JobExecutionStatusDetails</td>
<td>A collection of name/value pairs that describe the status of the job execution.</td>
</tr>
<tr>
<td>detailsMap</td>
<td>map</td>
<td>The job execution status.</td>
</tr>
<tr>
<td>thingArn</td>
<td>string</td>
<td>The ARN of the thing on which the job execution is running.</td>
</tr>
</tbody>
</table>
### Job Management and Control API

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>queuedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job execution was queued.</td>
</tr>
<tr>
<td>startedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job execution started.</td>
</tr>
<tr>
<td>lastUpdatedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job execution was last updated.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>long</td>
<td>A string (consisting of the digits &quot;0&quot; through &quot;9&quot;) which identifies this particular job execution on this particular device. It can be used in commands which return or update job execution information.</td>
</tr>
<tr>
<td>versionNumber</td>
<td>long</td>
<td>The version of the job execution. Job execution versions are incremented each time they are updated by a device.</td>
</tr>
</tbody>
</table>

**MQTT (7)**

Not available.

**GetJobDocument**

GetJobDocument command

Gets the job document for a job.

**Note**

Placeholder URLs are not replaced with presigned Amazon S3 URLs in the document returned. Presigned URLs are generated only when Jobs receives a request over MQTT.

**HTTPS (8)**

Request:

```
GET /jobs/jobId/job-document
```

jobId

The unique identifier you assigned to this job when it was created.

Response:

```
{
   "document": "string"
}
```
document

The job document content.

CLI (8)

Synopsis:

```bash
aws iot get-job-document \\
--job-id <value> \\
[--cli-input-json <value>] \\
[--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "jobId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>length max:64 min:1 pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
  "document": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>document</td>
<td>string</td>
<td>The job document content.</td>
</tr>
<tr>
<td></td>
<td>length max:32768</td>
<td></td>
</tr>
</tbody>
</table>

MQTT (8)

Not available.

**ListJobExecutionsForJob**

ListExecutionsForJob command

Gets a list of job executions for a job.
HTTPS (9)

Request:

```
GET /jobs/jobId/things?status=status&maxResults=maxResults&nextToken=nextToken
```

**jobId**

The unique identifier you assigned to this job when it was created.

**status**

Optional. A filter that lets you search for jobs that have the specified status: QUEUED, IN_PROGRESS, SUCCESS, FAILED, REJECTED, REMOVED, or CANCELED.

**maxResults**

Optional. The maximum number of results to be returned per request.

**nextToken**

Optional. The token to retrieve the next set of results.

Response:

```
{
  "executionSummaries": [ JobExecutionSummary ... ]
}
```

**executionSummaries**

A list of JobExecutionSummary (p. 308) objects associated with the specified job ID.

CLI (9)

**Synopsis:**

```
aws iot list-job-executions-for-job \ 
  --job-id <value> \ 
  [--status <value>] \ 
  [--max-results <value>] \ 
  [--next-token <value>] \ 
  [--cli-input-json <value>] \ 
  [--generate-cli-skeleton]
```

**cli-input-json format:**

```
{
  "jobId": "string",
  "status": "string",
  "maxResults": "integer",
  "nextToken": "string"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>pattern: [a-zA-Z0-9_]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the job.</td>
</tr>
<tr>
<td></td>
<td>enum: QUEUED</td>
<td>IN_PROGRESS</td>
</tr>
<tr>
<td>java class:</td>
<td>com.amazonaws.iot.laser.common.JobExecutionStatus</td>
<td></td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to be returned per request.</td>
</tr>
<tr>
<td>java class:</td>
<td>java.lang.Integer</td>
<td></td>
</tr>
<tr>
<td>range- max:250 min:1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token to retrieve the next set of results.</td>
</tr>
</tbody>
</table>

Output:

```json
{
   "executionSummaries": [
   {
       "thingArn": "string",
       "jobExecutionSummary": {
       "status": "string",
       "queuedAt": "timestamp",
       "startedAt": "timestamp",
       "lastUpdatedAt": "timestamp",
       "executionNumber": "long"
       }
   },
   "nextToken": "string"
   }
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>executionSummaries</td>
<td>list</td>
<td>A list of job execution summaries.</td>
</tr>
<tr>
<td>thingArn</td>
<td>string</td>
<td>The ARN of the thing on which the job execution is running.</td>
</tr>
<tr>
<td>jobExecutionSummary</td>
<td>JobExecutionSummary</td>
<td>Contains a subset of information about a job execution.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the job execution.</td>
</tr>
<tr>
<td></td>
<td>enum: QUEUED</td>
<td>The time, in milliseconds since the epoch, when the job execution was queued.</td>
</tr>
<tr>
<td></td>
<td>IN_PROGESS</td>
<td>The time, in milliseconds since the epoch, when the job execution started.</td>
</tr>
<tr>
<td></td>
<td>SUCCEEDED</td>
<td>The time, in milliseconds since the epoch, when the job execution was last updated.</td>
</tr>
<tr>
<td></td>
<td>FAILED</td>
<td>A string (consisting of the digits &quot;0&quot; through &quot;9&quot;) which identifies this particular job execution on this particular device. It can be used later in commands which return or update job execution information.</td>
</tr>
<tr>
<td></td>
<td>REJECTED</td>
<td>The token for the next set of results, or null if there are no additional results.</td>
</tr>
<tr>
<td></td>
<td>REMOVED</td>
<td>The token for the next set of results, or null if there are no additional results.</td>
</tr>
<tr>
<td></td>
<td>CANCELED</td>
<td>The token for the next set of results, or null if there are no additional results.</td>
</tr>
<tr>
<td>queuedAt</td>
<td>timestamp</td>
<td>The status of the job execution.</td>
</tr>
<tr>
<td>startedAt</td>
<td>timestamp</td>
<td>The status of the job execution.</td>
</tr>
<tr>
<td>lastUpdatedAt</td>
<td>timestamp</td>
<td>The status of the job execution.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>long</td>
<td>The status of the job execution.</td>
</tr>
<tr>
<td></td>
<td>java class:</td>
<td>The status of the job execution.</td>
</tr>
</tbody>
</table>

MQTT (9)

Not available.

**ListJobExecutionsForThing**

ListJobExecutionsForThing command

 Gets a list of job executions for a thing.

**HTTPS (10)**

Request:

```
GET /things/thingName/jobs?status=status&maxResults=maxResults&nextToken=nextToken
```

thingName

The name of the thing for which JobExecutions will be listed.
status

An optional filter that lets you search for jobs that have the specified status: QUEUED, IN_PROGRESS, SUCCESS, FAILED, REJECTED, REMOVED, or CANCELED.

maxResults

The maximum number of results to be returned per request.

nextToken

The token for the next set of results, or null if there are no additional results.

Response:

```
{
  "executionSummaries": [JobExecutionSummary ... ]
}
```

executionSummaries

A list of the JobExecutionSummary (p. 308) objects for the job executions associated with the specified thing.

CLI (10)

Synopsis:

```
aws iot list-job-executions-for-thing \
  --thing-name <value> \
  [--status <value>] \
  [--max-results <value>] \
  [--next-token <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "thingName": "string",
  "status": "string",
  "maxResults": "integer",
  "nextToken": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The thing name.</td>
</tr>
<tr>
<td></td>
<td>length max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>An optional filter that lets you search for jobs that have the specified status.</td>
</tr>
<tr>
<td></td>
<td>enum: QUEUED</td>
<td>IN_PROGRESS</td>
</tr>
</tbody>
</table>
AWS IoT Developer Guide
Job Management and Control API

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td>FAILED</td>
<td>REJECTED</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to be returned per request.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token to retrieve the next set of results.</td>
</tr>
</tbody>
</table>

Output:

```json
{
  "executionSummaries": [
    {
      "jobId": "string",
      "jobExecutionSummary": {
        "status": "string",
        "queuedAt": "timestamp",
        "startedAt": "timestamp",
        "lastUpdatedAt": "timestamp",
        "executionNumber": "long"
      }
    },
    {
      "jobId": "string",
      "jobExecutionSummary": {
        "status": "string",
        "queuedAt": "timestamp",
        "startedAt": "timestamp",
        "lastUpdatedAt": "timestamp",
        "executionNumber": "long"
      }
    }
  ],
  "nextToken": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>executionSummaries</td>
<td>list</td>
<td>A list of job execution summaries.</td>
</tr>
<tr>
<td>memberId</td>
<td>JobExecutionSummaryForThing</td>
<td>jobId</td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td>length max:64 min:1</td>
</tr>
<tr>
<td></td>
<td>jobId</td>
<td>pattern: [a-zA-Z0-9_-]+</td>
</tr>
<tr>
<td></td>
<td>JobExecutionSummaryForThing</td>
<td></td>
</tr>
<tr>
<td>jobExecutionSummary</td>
<td>JobExecutionSummary</td>
<td>Contains a subset of information about a job execution.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the job execution.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
</tbody>
</table>

**MQTT (10)**

Not available.

**ListJobs**

**ListJobs command**

Gets a list of the jobs in your AWS account.

**HTTPS (11)**

Request:

```plaintext
GET /jobs?
status=status&targetSelection=targetSelection&thingGroupName=thingGroupName&thingGroupId=thingGroupId&maxResults=maxResults&nextToken=nextToken
```

**status**

Optional. A filter that lets you search for jobs that have the specified status: IN_PROGRESS, CANCELED, or COMPLETED.
targetSelection

Optional. A filter that lets you search for jobs that have the specified targetSelection value: CONTINUOUS or SNAPSHOT.

thingGroupName

Optional. A filter that lets you search for jobs that have the specified thing group name as a target.

thingGroupId

Optional. A filter that lets you search for jobs that have the specified thing group ID as a target.

maxResults

Optional. The maximum number of results to be returned per request.

nextToken

Optional. The token to retrieve the next set of results.

Response:

```
{
  "jobs": [ JobSummary ... ],
}
```

jobs

A list of JobSummary (p. 306) objects, one for each job in your AWS account that matches the specified filtering criteria.

CLI (11)

Synopsis:

```
aws iot list-jobs \ 
  [--status <value>] \ 
  [--target-selection <value>] \ 
  [--max-results <value>] \ 
  [--next-token <value>] \ 
  [--thing-group-name <value>] \ 
  [--thing-group-id <value>] \ 
  [--cli-input-json <value>] \ 
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "status": "string",
  "targetSelection": "string",
  "maxResults": "integer",
  "nextToken": "string",
  "thingGroupName": "string",
  "thingGroupId": "string"
}
```
cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>string</td>
<td>An optional filter that lets you search for jobs that have the specified status.</td>
</tr>
<tr>
<td></td>
<td>enum: IN_PROGRESS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CANCELED</td>
<td></td>
</tr>
<tr>
<td></td>
<td>COMPLETED</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class:</td>
<td>ccom.amazonaws.iot.laser.common.JobStatus</td>
</tr>
<tr>
<td>targetSelection</td>
<td>string</td>
<td>Specifies whether the job will continue to run (CONTINUOUS), or will be complete after all those things specified as targets have completed the job (SNAPSHOT). If continuous, the job may also be run on a thing when a change is detected in a target. For example, a job will run on a thing when the thing is added to a target group, even after the job was completed by all things originally in the group.</td>
</tr>
<tr>
<td></td>
<td>enum: CONTINUOUS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNAPSHOT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class:</td>
<td>com.amazonaws.iot.laser.TargetSelection</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return per request.</td>
</tr>
<tr>
<td></td>
<td>java class:</td>
<td>java.lang.Integer</td>
</tr>
<tr>
<td></td>
<td>range- max:250</td>
<td>min:1</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>thingGroupName</td>
<td>string</td>
<td>A filter that limits the returned jobs to those for the specified group.</td>
</tr>
<tr>
<td></td>
<td>length max:128</td>
<td>min:1</td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>thingGroupId</td>
<td>string</td>
<td>A filter that limits the returned jobs to those for the specified group.</td>
</tr>
<tr>
<td></td>
<td>length max:128</td>
<td>min:1</td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
    "jobs": [ 
    {
        "jobArn": "string",
        "jobId": "string",
        "thingGroupId": "string",
        "targetSelection": "string",
        "status": "string",
        "createdAt": "timestamp",
```
"lastUpdatedAt": "timestamp",
"completedAt": "timestamp"
}
],
"nextToken": "string"
}

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobs</td>
<td>list</td>
<td>A list of jobs.</td>
</tr>
<tr>
<td></td>
<td>member: JobSummary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>JobSummary</td>
<td>JobSummary</td>
<td></td>
</tr>
<tr>
<td>jobArn</td>
<td>string</td>
<td>The job ARN.</td>
</tr>
<tr>
<td>jobld</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>length max:64 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>thingGroupId</td>
<td>string</td>
<td>The ID of the thing group.</td>
</tr>
<tr>
<td></td>
<td>length max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-]++</td>
<td></td>
</tr>
<tr>
<td>targetSelection</td>
<td>string</td>
<td>Specifies whether the job will continue to run (CONTINUOUS), or will be complete after all those things specified as targets have completed the job (SNAPSHOT). If continuous, the job may also be run on a thing when a change is detected in a target. For example, a job will run on a thing when the thing is added to a target group, even after the job was completed by all things originally in the group.</td>
</tr>
<tr>
<td></td>
<td>enum: CONTINUOUS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNAPSHOT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>com.amazonaws.iot.laser TargetsSelection</td>
<td></td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The job summary status.</td>
</tr>
<tr>
<td></td>
<td>enum: IN_PROGRESS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CANCELED</td>
<td></td>
</tr>
<tr>
<td></td>
<td>COMPLETED</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>com.amazonaws.iot.laser.common.JobStatus</td>
<td></td>
</tr>
<tr>
<td>createdAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job was created.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>lastUpdatedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job was last updated.</td>
</tr>
<tr>
<td>completedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job completed.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

MQTT (11)
Not available.

Jobs Device MQTT and HTTPS APIs

Device MQTT and HTTPS Data Types

The following data types are used to communicate with Jobs over the MQTT and HTTPS protocols.

JobExecution

JobExecution data type

Contains data about a job execution.

syntax (7)

```json
{
  "jobId" : "string",
  "thingName" : "string",
  "jobDocument" : "string",
  "status": "QUEUED|IN_PROGRESS|FAILED|SUCCESS|CANCELED|REJECTED|REMOVED",
  "statusDetails": {
    "string": "string"
  },
  "queuedAt" : "timestamp",
  "startedAt" : "timestamp",
  "lastUpdatedAt" : "timestamp",
  "versionNumber" : "number",
  "executionNumber": "long"
}
```

description (7)

jobId

The unique identifier you assigned to this job when it was created.

thingName

The name of the thing that is executing the job.

jobDocument

The content of the job document.
status

The status of the job execution. Can be one of: "QUEUED", "IN_PROGRESS", "FAILED", "SUCCESS", "CANCELED", "REJECTED", or "REMOVED".

statusDetails

A collection of name/value pairs that describe the status of the job execution.

queuedAt

The time, in milliseconds since the epoch, when the job execution was enqueued.

startedAt

The time, in milliseconds since the epoch, when the job execution was started.

canceledAt

The time, in milliseconds since the epoch, when the job execution was last updated.

versionNumber

The version of the job execution. Job execution versions are incremented each time they are updated by a device.

canceledAt

A number that identifies a particular job execution on a particular device. It can be used later in commands that return or update job execution information.

**JobExecutionState**

JobExecutionState data type

Contains data about the state of a job execution.

**syntax (8)**

```json
{
  "status": "QUEUED|IN_PROGRESS|FAILED|SUCCESS|CANCELED|REJECTED|REMOVED",
  "statusDetails": {
    "string": "string"
  }
}
```

**description (8)**

**status**

The status of the job execution. Can be one of: "QUEUED", "IN_PROGRESS", "FAILED", "SUCCESS", "CANCELED", "REJECTED", or "REMOVED".

**statusDetails**

A collection of name/value pairs that describe the status of the job execution.

**versionNumber**

The version of the job execution. Job execution versions are incremented each time they are updated by a device.
JobExecutionSummary

JobExecutionSummary data type

Contains a subset of information about a job execution.

.syntax (9)

```
{
    "jobId": "string",
    "queuedAt": timestamp,
    "startedAt": timestamp,
    "lastUpdatedAt": timestamp,
    "versionNumber": "number",
    "executionNumber": "long"
}
```

description (9)

jobId

The unique identifier you assigned to this job when it was created.

queuedAt

The time, in milliseconds since the epoch, when the job execution was enqueued.

startedAt

The time, in milliseconds since the epoch, when the job execution started.

lastUpdatedAt

The time, in milliseconds since the epoch, when the job execution was last updated.

versionNumber

The version of the job execution. Job execution versions are incremented each time AWS IoT Jobs receives an update from a device.

executionNumber

A number that identifies a particular job execution on a particular device.

ErrorResponse

ErrorResponse data type

Contains information about an error that occurred during a Jobs operation.

.syntax (10)

```
{
    "code": "ErrorCode",
    "message": "string",
    "clientToken": "string",
    "timestamp": timestamp,
    "executionState": JobExecutionState
}
```

description (10)

code

ErrorCode can be set to:
InvalidTopic

The request was sent to a topic in the Jobs namespace that does not map to any API.

InvalidJson

The contents of the request could not be interpreted as valid UTF-8-encoded JSON.

InvalidRequest

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

InvalidStateTransition

An update attempted to change the job execution to a state that is invalid because of the job execution's current state (for example, an attempt to change a request in state SUCCESS to state IN_PROGRESS). In this case, the body of the error message also contains the executionState field.

ResourceNotFound

The JobExecution specified by the request topic does not exist.

VersionMismatch

The expected version specified in the request does not match the version of the job execution in Jobs. In this case, the body of the error message also contains the executionState field.

InternalError

There was an internal error processing the request.

RequestThrottled

The request was throttled.

TerminalStateReached

Occurs when a command to describe a job is performed on a job that is in a terminal state.

message

An error message string.

clientToken

An arbitrary string used to correlate a request with its reply.

timestamp

The time, in milliseconds since the epoch.

executionState

A JobExecutionState (p. 347) object. This field is included only when the code field has the value InvalidStateTransition or VersionMismatch. This makes it unnecessary in these cases to perform a separate DescribeJobExecution request to obtain the current job execution status data.

Device Commands

The following commands are available over the MQTT and HTTPS protocols.
**GetPendingJobExecutions**

GetPendingJobExecutions command

Gets the list of all jobs for a thing that are not in a terminal state.

**MQTT (12)**

To invoke this API, publish a message on `$aws/things/thingName/jobs/get`.

Request payload:

```json
{  "clientToken": "string" }
```

clientToken

Optional. A client token used to correlate requests and responses. Enter an arbitrary value here and it will be reflected in the response.

To receive the response, subscribe to:

- `$aws/things/thingName/jobs/get/accepted` and...
- `$aws/things/thingName/jobs/get/rejected` or...
- `$aws/things/thingName/jobs/get/` for both...

Response payload:

```json
{
  "inProgressJobs" : [ JobExecutionSummary ... ],
  "queuedJobs" : [ JobExecutionSummary ... ],
  "timestamp" : 1489096425069,
  "clientToken" : "client-001"
}
```

**inProgressJobs**

A list of JobExecutionSummary (p. 348) objects with status IN_PROGRESS.

**queuedJobs**

A list of JobExecutionSummary (p. 348) objects with status QUEUED.

**clientToken**

A client token used to correlate requests and responses.

**timestamp**

The time, in milliseconds since the epoch, when the message was sent.

**HTTPS (12)**

Request:

```plaintext
GET /things/thingName/jobs
```

**thingName**

The name of the thing associated with the device.
Response:

```json
{
    "inProgressJobs": [ JobExecutionSummary ... ],
    "queuedJobs": [ JobExecutionSummary ... ]
}
```

**inProgressJobs**

A list of JobExecutionSummary (p. 348) objects.

**queuedJobs**

A list of JobExecutionSummary (p. 348) objects.

**CLI (12)**

**Synopsis:**

```bash
aws iot-jobs-data get-pending-job-executions \
    --thing-name <value> \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
    "thingName": "string"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing that is executing the job.</td>
</tr>
<tr>
<td></td>
<td>length max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
</tbody>
</table>
"versionNumber": "long",
"executionNumber": "long"
}
]
}

### cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inProgressJobs</td>
<td>list</td>
<td>A list of JobExecutionSummary objects with status IN_PROGRESS.</td>
</tr>
<tr>
<td></td>
<td>member:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>JobExecutionSummary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class:</td>
<td>java.util.List</td>
</tr>
<tr>
<td>JobExecutionSummary</td>
<td>JobExecutionSummary</td>
<td></td>
</tr>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>length max:64 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>queuedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was enqueued.</td>
</tr>
<tr>
<td>startedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution started.</td>
</tr>
<tr>
<td></td>
<td>java class:</td>
<td>java.lang.Long</td>
</tr>
<tr>
<td>lastUpdatedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was last updated.</td>
</tr>
<tr>
<td>versionNumber</td>
<td>long</td>
<td>The version of the job execution. Job execution versions are incremented each time AWS IoT Jobs receives an update from a device.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>long</td>
<td>A number that identifies a particular job execution on a particular device.</td>
</tr>
<tr>
<td></td>
<td>java class:</td>
<td>java.lang.Long</td>
</tr>
<tr>
<td>queuedJobs</td>
<td>list</td>
<td>A list of JobExecutionSummary objects with status QUEUED.</td>
</tr>
<tr>
<td></td>
<td>member:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>JobExecutionSummary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class:</td>
<td>java.util.List</td>
</tr>
<tr>
<td>JobExecutionSummary</td>
<td>JobExecutionSummary</td>
<td></td>
</tr>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>length max:64 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>queuedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was enqueued.</td>
</tr>
<tr>
<td>startedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution started.</td>
</tr>
<tr>
<td>startedAt</td>
<td>java class: java.lang.Long</td>
<td>The time, in milliseconds since the epoch, when the job execution started.</td>
</tr>
<tr>
<td>lastUpdatedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was last updated.</td>
</tr>
<tr>
<td>versionNumber</td>
<td>long</td>
<td>The version of the job execution. Job execution versions are incremented each time AWS IoT Jobs receives an update from a device.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>long</td>
<td>A number that identifies a particular job execution on a particular device.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>java class: java.lang.Long</td>
<td>A number that identifies a particular job execution on a particular device.</td>
</tr>
</tbody>
</table>

**StartNextPendingJobExecution**

StartNextPendingJobExecution command

- Gets and starts the next pending (status IN_PROGRESS or QUEUED) job execution for a thing.
  - Any job executions with status IN_PROGRESS are returned first.
  - Job executions are returned in the order in which they were created.
  - If the next pending job execution is QUEUED, its state is changed to IN_PROGRESS and the job execution's status details are set as specified.
  - If the next pending job execution is already IN_PROGRESS, its status details are not changed.
  - If no job executions are pending, the response does not include the execution field.

**MQTT (13)**

To invoke this API, publish a message on: `$aws/things/thingName/jobs/start-next`.

Request payload:

```json
{
  "statusDetails": {
    "string": "job-execution-state"
  },
  "clientToken": "string"
}
```

**statusDetails**

A collection of name/value pairs that describe the status of the job execution. If not specified, the statusDetails are unchanged.
clientToken

A client token used to correlate requests and responses. Enter an arbitrary value here and it will be reflected in the response.

To receive the response, subscribe to:

- $aws/things/thingName/jobs/start-next/accepted ...and...
- $aws/things/thingName/jobs/start-next/rejected ...or...
- $aws/things/thingName/jobs/start-next/# ...for both...

Response payload:

```json
{
  "execution": JobExecutionData,
  "timestamp": timestamp,
  "clientToken": "string"
}
```

execution

A JobExecution (p. 346) object. For example:

```json
{
  "execution": {
    "jobId": "022",
    "thingName": "MyThing",
    "jobDocument": "< contents of job document >",
    "status": "IN_PROGRESS",
    "queuedAt": 1489096123309,
    "lastUpdatedAt": 1489096123309,
    "versionNumber": 1,
    "executionNumber": 1234567890
  },
  "clientToken": "client-1",
  "timestamp": 1489088524284,
}
```

timestamp

The time, in milliseconds since the epoch, when the message was sent to the device.

clientToken

A client token used to correlate requests and responses.

HTTPS (13)

Request:

```plaintext
PUT /things/thingName/jobs/$next
{
  "statusDetails": {
    "string": "string"
  }
}
```
thingName
   The name of the thing associated with the device.
statusDetails
   A collection of name/value pairs that describe the status of the job execution. If not specified, the statusDetails are unchanged.

Response:

```json
{
   "execution" : JobExecution
}
```

execution

A JobExecution (p. 346) object. For example:

```json
{
   "execution" : {
      "jobId" : "022",
      "thingName" : "MyThing",
      "jobDocument" : "< contents of job document >",
      "status" : "IN_PROGRESS",
      "queuedAt" : 1489096123309,
      "lastUpdatedAt" : 1489096123309,
      "versionNumber" : 1,
      "executionNumber" : 1234567890
   },
   "clientToken" : "client-1",
   "timestamp" : 1489088524284,
}
```

CLI (13)

**Synopsis:**

```
aws iot-jobs-data start-next-pending-job-execution \  
   --thing-name <value> \  
   [--status-details <value>] \  
   [--cli-input-json <value>] \  
   [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
   "thingName": "string",
   "statusDetails": {
      "string": "string"
   }
}
```

**cli-input-json fields:**

<p>| Name          | Type   | Description                                               |
|---------------|--------|---------------|----------------------------------------------------------|
| thingName     | string | The name of the thing associated with the device.        |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>length max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_:-]+</td>
<td></td>
</tr>
<tr>
<td>statusDetails</td>
<td>map</td>
<td>A collection of name/value pairs that describe the status of the job execution. If not specified, the statusDetails are unchanged.</td>
</tr>
<tr>
<td>DetailsKey</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td></td>
<td>length max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_:-]+</td>
<td></td>
</tr>
<tr>
<td>DetailsValue</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td></td>
<td>length max:1024 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [^\p{C}]*+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
    "execution": {
        "jobId": "string",
        "thingName": "string",
        "status": "string",
        "statusDetails": {
            "string": "string"
        },
        "queuedAt": "long",
        "startedAt": "long",
        "lastUpdatedAt": "long",
        "versionNumber": "long",
        "executionNumber": "long",
        "jobDocument": "string"
    }
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>execution</td>
<td>JobExecution</td>
<td>A JobExecution object.</td>
</tr>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>length max:64 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_:-]+</td>
<td></td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing that is executing the job.</td>
</tr>
<tr>
<td></td>
<td>length max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_:-]+</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the job execution. Can be one of: &quot;QUEUED&quot;, &quot;IN_PROGRESS&quot;, &quot;SUCCESSED&quot;, &quot;FAILED&quot;, &quot;SUCCESS&quot;, &quot;CANCELED&quot;, &quot;REJECTED&quot;, or &quot;REMOVED&quot;.</td>
</tr>
<tr>
<td>statusDetails</td>
<td>map</td>
<td>A collection of name/value pairs that describe the status of the job execution.</td>
</tr>
<tr>
<td>DetailsKey</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td></td>
<td>length max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>DetailsValue</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td></td>
<td>length max:1024 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [^\p{C}]*+</td>
<td></td>
</tr>
<tr>
<td>queuedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was enqueued.</td>
</tr>
<tr>
<td>startedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was started.</td>
</tr>
<tr>
<td></td>
<td>java class: java.lang.Long</td>
<td></td>
</tr>
<tr>
<td>lastUpdatedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was last updated.</td>
</tr>
<tr>
<td>versionNumber</td>
<td>long</td>
<td>The version of the job execution. Job execution versions are incremented each time they are updated by a device.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>long</td>
<td>A number that identifies a particular job execution on a particular device. It can be used later in commands that return or update job execution information.</td>
</tr>
<tr>
<td></td>
<td>java class: java.lang.Long</td>
<td></td>
</tr>
<tr>
<td>jobDocument</td>
<td>string</td>
<td>The content of the job document.</td>
</tr>
<tr>
<td></td>
<td>length max:32768</td>
<td></td>
</tr>
</tbody>
</table>
DescribeJobExecution

DescribeJobExecution command

Gets detailed information about a job execution.

You can set the jobId to $next to return the next pending (status IN_PROGRESS or QUEUED) job execution for a thing.

MQTT (14)

To invoke this API, publish a message on $aws/things/thingName/jobs/jobId/get.

Request payload:

```json
{
   "executionNumber": "long",
   "includeJobDocument": "boolean",
   "clientToken": "string"
}
```

tingName

The name of the thing associated with the device.

jobId

The unique identifier assigned to this job when it was created.

Or use $next to return the next pending (status IN_PROGRESS or QUEUED) job execution for a thing. In this case, any job executions with status IN_PROGRESS are returned first. Job executions are returned in the order in which they were created.

executionNumber

Optional. A number that identifies a particular job execution on a particular device. If not specified, the latest job execution is returned.

includeJobDocument

Optional. When set to true, the response contains the job document. The default is true.

clientToken

A client token used to correlate requests and responses. Enter an arbitrary value here and it will be reflected in the response.

To receive the response, subscribe to:

- $aws/things/thingName/jobs/jobId/get/accepted ...
- $aws/things/thingName/jobs/jobId/get/rejected ...
- $aws/things/thingName/jobs/jobId/get/# ...

Response payload:

```json
{
   "execution" : JobExecutionData,
   "timestamp": "timestamp",
   "clientToken": "string"
}
```
execution

A JobExecution (p. 346) object.

timestamp

The time, in milliseconds since the epoch, when the message was sent.

clientToken

A client token used to correlate requests and responses.

HTTPS (14)

The job’s execution status must be QUEUED or IN_PROGRESS.

Request:

```
GET /things/thingName/jobs/jobId?
  executionNumber=executionNumber&includeJobDocument=includeJobDocument
```

thingName

The name of the thing associated with the device.

jobId

The unique identifier assigned to this job when it was created.

Or use $next to return the next pending (status IN_PROGRESS or QUEUED) job execution for a thing. In this case, any job executions with status IN_PROGRESS are returned first. Job executions are returned in the order in which they were created.

includeJobDocument

Optional. When set to true, the response contains the job document. The default is false.

executionNumber

Optional. A number that identifies a particular job execution on a particular device. If not specified, the latest job execution is returned.

Response:

```
{
  "execution" : JobExecution,
}
```

execution

A JobExecution (p. 346) object.

CLI (14)

The job’s execution status must be QUEUED or IN_PROGRESS.

**Synopsis:**

```
aws iot-jobs-data describe-job-execution \
  --job-id <value> \
```
--thing-name <value> \
[--include-job-document | --no-include-job-document] \
[--execution-number <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]

cli-input-json format:
{
  "jobId": "string",
  "thingName": "string",
  "includeJobDocument": "boolean",
  "executionNumber": "long"
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier assigned to this job when it was created, or $next to return the next pending (status IN_PROGRESS or QUEUED) job execution for a thing. In this case, any job executions with status IN_PROGRESS are returned first. Job executions are returned in the order in which they were created.</td>
</tr>
<tr>
<td>thingName</td>
<td>string, length max:128 min:1</td>
<td>The thing name associated with the device the job execution is running on.</td>
</tr>
<tr>
<td>includeJobDocument</td>
<td>boolean, java class: java.lang.Boolean</td>
<td>Optional. When set to true, the response contains the job document. The default is false.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>long, java class: java.lang.Long</td>
<td>Optional. A number that identifies a particular job execution on a particular device. If not specified, the latest job execution is returned.</td>
</tr>
</tbody>
</table>

Output:
{
  "execution": {
    "jobId": "string",
    "thingName": "string",
    "status": "string",
    "statusDetails": {
      "string": "string"
    },
    "queuedAt": "long",
    "startedAt": "long",
    ...
  }
}
"lastUpdatedAt": "long",
"versionNumber": "long",
"executionNumber": "long",
"jobDocument": "string"
}
}

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>execution</td>
<td>JobExecution</td>
<td>Contains data about a job execution.</td>
</tr>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing that is executing the job.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the job execution. Can be one of: &quot;QUEUED&quot;, &quot;IN_PROGRESS&quot;, &quot;FAILED&quot;, &quot;SUCCESS&quot;, &quot;CANCELED&quot;, &quot;REJECTED&quot;, or &quot;REMOVED&quot;.</td>
</tr>
<tr>
<td>statusDetails</td>
<td>map</td>
<td>A collection of name/value pairs that describe the status of the job execution.</td>
</tr>
<tr>
<td>DetailsKey</td>
<td>string</td>
<td>The time, in milliseconds since the epoch, when the job execution was enqueued.</td>
</tr>
<tr>
<td>DetailsValue</td>
<td>string</td>
<td>The time, in milliseconds since the epoch, when the job execution was started.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>lastUpdatedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was last updated.</td>
</tr>
<tr>
<td>versionNumber</td>
<td>long</td>
<td>The version of the job execution. Job execution versions are incremented each time they are updated by a device.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>long java class: java.lang.Long</td>
<td>A number that identifies a particular job execution on a particular device. It can be used later in commands that return or update job execution information.</td>
</tr>
<tr>
<td>jobDocument</td>
<td>string length max:32768</td>
<td>The content of the job document.</td>
</tr>
</tbody>
</table>

### UpdateJobExecution

**UpdateJobExecution command**

Updates the status of a job execution.

MQTT (15)

To invoke this API, publish a message on `$aws/things/thingName/jobs/jobId/update`.

Request payload:

```json
{
  "status": "job-execution-state",
  "statusDetails": {
    "string": "string"
  },
  "expectedVersion": "number",
  "executionNumber": "long",
  "includeJobExecutionState": "boolean",
  "includeJobDocument": "boolean",
  "clientToken": "string"
}
```

**status**

The new status for the job execution (IN_PROGRESS, FAILED, SUCCEEDED, or REJECTED). This must be specified on every update.

**statusDetails**

A collection of name/value pairs that describe the status of the job execution. If not specified, the statusDetails are unchanged.

**expectedVersion**

The expected current version of the job execution. Each time you update the job execution, its version is incremented. If the version of the job execution stored in Jobs does not match,
the update is rejected with a VersionMismatch error, and an ErrorResponse (p. 348) that contains the current job execution status data is returned. (This makes it unnecessary to perform a separate DescribeJobExecution request in order to obtain the job execution status data.)

**executionNumber**

Optional. A number that identifies a particular job execution on a particular device. If not specified, the latest job execution is used.

**includeJobExecutionState**

Optional. When included and set to true, the response contains the JobExecutionState field. The default is false.

**includeJobDocument**

Optional. When included and set to true, the response contains the JobDocument. The default is false.

**clientToken**

A client token used to correlate requests and responses. Enter an arbitrary value here and it will be reflected in the response.

To receive the response, subscribe to:

- `$aws/things/thingName/jobs/jobId/update/accepted` ...and...
- `$aws/things/thingName/jobs/jobId/update/rejected` ...or...
- `$aws/things/thingName/jobs/jobId/update/#` ...for both...

**Response payload:**

```
{
    "executionState": JobExecutionState,
    "jobDocument": "string",
    "timestamp": timestamp,
    "clientToken": "string"
}
```

**executionState**

A JobExecutionState (p. 347) object.

**jobDocument**

A job document (p. 281) object.

**timestamp**

The time, in milliseconds since the epoch, when the message was sent.

**clientToken**

A client token used to correlate requests and responses.

**HTTPS (15)**

**Request:**

```
POST /things/thingName/jobs/jobId
{
```
"status": "job-execution-state",
"statusDetails": {,
   "string": "string"
   ...
},
"expectedVersion": "number",
"includeJobExecutionState": "boolean",
"includeJobDocument": "boolean",
"executionNumber": "long"
}

thingName

The name of the thing associated with the device.

jobId

The unique identifier assigned to this job when it was created.

status

The new status for the job execution (IN_PROGRESS, FAILED, SUCCEEDED, or REJECTED). This must be specified on every update.

statusDetails

Optional. A collection of name/value pairs that describe the status of the job execution. If not specified, the statusDetails are unchanged.

expectedVersion

Optional. The expected current version of the job execution. Each time you update the job execution, its version is incremented. If the version of the job execution stored in Jobs does not match, the update is rejected with a VersionMismatch error, and an ErrorResponse (p. 348) that contains the current job execution status data is returned. (This makes it unnecessary to perform a separate DescribeJobExecution request in order to obtain the job execution status data.)

includeJobExecutionState

Optional. When included and set to true, the response contains the JobExecutionState data. The default is false.

includeJobDocument

Optional. When set to true, the response contains the job document. The default is false.

executionNumber

Optional. A number that identifies a particular job execution on a particular device.

Response:

{
   "executionState": JobExecutionState,
   "jobDocument": "string"
}

executionState

A JobExecutionState (p. 347) object.

jobDocument

The contents of the job document (p. 281).
CLI (15)

Synopsis:

```
aws iot-jobs-data update-job-execution
   --job-id <value> \
   --thing-name <value> \
   --status <value> \
   [--status-details <value>] \
   [--expected-version <value>] \
   [--include-job-execution-state | --no-include-job-execution-state] \
   [--include-job-document | --no-include-job-document] \
   [--execution-number <value>] \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "jobId": "string",
   "thingName": "string",
   "status": "string",
   "statusDetails": {
      "string": "string"
   },
   "expectedVersion": "long",
   "includeJobExecutionState": "boolean",
   "includeJobDocument": "boolean",
   "executionNumber": "long"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>length max:64 min:1</td>
<td>The unique identifier assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td>The unique identifier assigned to this job when it was created.</td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing associated with the device.</td>
</tr>
<tr>
<td></td>
<td>length max:128 min:1</td>
<td>The name of the thing associated with the device.</td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td>The name of the thing associated with the device.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The new status for the job execution (IN_PROGRESS, FAILED, SUCCESS, or REJECTED). This must be specified on every update.</td>
</tr>
<tr>
<td></td>
<td>enum: QUEUED</td>
<td>IN_PROGRESS</td>
</tr>
<tr>
<td>statusDetails</td>
<td>map</td>
<td>Optional. A collection of name/value pairs that describe the status of the job execution. If</td>
</tr>
<tr>
<td></td>
<td>key: DetailsKey</td>
<td>Optional. A collection of name/value pairs that describe the status of the job execution. If</td>
</tr>
<tr>
<td></td>
<td>value: DetailsValue</td>
<td>Optional. A collection of name/value pairs that describe the status of the job execution. If</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>not specified, the statusDetails are unchanged.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DetailsKey</td>
<td>string</td>
<td>length max:128 min:1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
</tr>
<tr>
<td>DetailsValue</td>
<td>string</td>
<td>length max:1024 min:1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pattern: [^\p{C}]*+</td>
</tr>
<tr>
<td>expectedVersion</td>
<td>long</td>
<td>java class: java.lang.Long</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional. The expected current version of the job execution. Each time you update the job execution, its version is incremented. If the version of the job execution stored in Jobs does not match, the update is rejected with a VersionMismatch error, and an ErrorResponse that contains the current job execution status data is returned. (This makes it unnecessary to perform a separate DescribeJobExecution request in order to obtain the job execution status data.)</td>
</tr>
<tr>
<td>includeJobExecutionState</td>
<td>boolean</td>
<td>Optional. When included and set to true, the response contains the JobExecutionState data. The default is false.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java class: java.lang.Boolean</td>
</tr>
<tr>
<td>includeJobDocument</td>
<td>boolean</td>
<td>Optional. When set to true, the response contains the job document. The default is false.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java class: java.lang.Boolean</td>
</tr>
<tr>
<td>executionNumber</td>
<td>long</td>
<td>java class: java.lang.Long</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional. A number that identifies a particular job execution on a particular device.</td>
</tr>
</tbody>
</table>

**Output:**

```json
{
  "executionState": {
    "status": "string",
    "statusDetails": {
      "string": "string"
    },
    "versionNumber": "long"
  }
}
```
"jobDocument": "string"
}

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>executionState</td>
<td>JobExecutionState</td>
<td>A JobExecutionState object.</td>
</tr>
<tr>
<td>status</td>
<td>string enum: QUEUED</td>
<td>The status of the job execution. Can be one of: &quot;QUEUED&quot;, &quot;IN_PROGRESS&quot;,</td>
</tr>
<tr>
<td></td>
<td>IN_PROGRESS</td>
<td>&quot;FAILED&quot;, &quot;SUCCEEDED&quot;, &quot;REJECTED&quot;, &quot;REMOVED&quot;, &quot;CANCELED&quot;.</td>
</tr>
<tr>
<td></td>
<td>java class:</td>
<td>com.amazonaws.iot.laser.common.JobExecutionStatus</td>
</tr>
<tr>
<td>statusDetails</td>
<td>map key: DetailsKey</td>
<td>A collection of name/value pairs that describe the status of the job execution.</td>
</tr>
<tr>
<td></td>
<td>value: DetailsValue</td>
<td></td>
</tr>
<tr>
<td>DetailsKey</td>
<td>string length max:128</td>
<td>The version of the job execution. Job execution versions are incremented</td>
</tr>
<tr>
<td></td>
<td>min:1 pattern: [a-zA-Z0-9:_-]+</td>
<td>each time they are incremented by a device.</td>
</tr>
<tr>
<td>DetailsValue</td>
<td>string length max:1024</td>
<td></td>
</tr>
<tr>
<td></td>
<td>min:1 pattern: [^\p{C}]*+</td>
<td></td>
</tr>
<tr>
<td>versionNumber</td>
<td>long</td>
<td></td>
</tr>
<tr>
<td>jobDocument</td>
<td>string length max:32768</td>
<td>The contents of the Job Documents.</td>
</tr>
</tbody>
</table>

**JobExecutionsChanged**

JobExecutionsChanged message

Sent whenever a job execution is added to or removed from the list of pending job executions for a thing.

MQTT (16)

Topic: $aws/things/thingName/jobs/notify

Message payload:

```json
{
```
"jobs" : {
    "JobExecutionState": [ JobExecutionSummary (p. 308) ... ]
},
"timestamp": timestamp,
}

HTTPS (16)
Not available.
CLI (16)
Not available.

NextJobExecutionChanged

NextJobExecutionChanged message

Sent whenever there is a change to which job execution is next on the list of pending job executions for a thing, as defined for DescribeJobExecution (p. 358) with jobId $next. This message is not sent when the next job's execution details change, only when the next job that would be returned by DescribeJobExecution with jobId $next has changed. Consider job executions J1 and J2 with state QUEUED. J1 is next on the list of pending job executions. If the state of J2 is changed to IN_PROGRESS while the state of J1 remains unchanged, then this notification is sent and contains details of J2.

MQTT (17)

Topic: $aws/things/thingName/jobs/notify-next

Message payload:

{
    "execution": JobExecutionData (p. 346),
    "timestamp": timestamp,
}

HTTPS (17)
Not available.
CLI (17)
Not available.

Job Limits

For job limit information, see AWS IoT Job Limits in the AWS General Reference.
Device Provisioning

AWS IoT device provisioning involves the creation and registration of the following entities:

- A certificate. You can provision a device with an existing certificate or have AWS IoT create and register one for you.
- A policy attached to the certificate.
- A unique identifier for the thing (device).
- A set of attributes for the thing, including existing thing types and groups.

To provision a device, create a template that describes the resources required for your device. Devices require a thing, a certificate, and one or more policies. A thing is an entry in the registry that contains attributes that describe the device. Devices use certificates to authenticate with AWS IoT. Policies determine which operations a device can perform in AWS IoT.

Templates contain variables that are replaced when the template is used to provision a device. A dictionary (map) is used to provide values for the variables used in a template. You can use the same template to provision multiple devices. You simply pass in different values for the template variables in the dictionary.

AWS IoT provides three ways to provision devices:

- Single-thing provisioning with a provisioning template. This is a good option if you only need to provision devices one at a time.
- Just-in-time provisioning (JITP) with a template that registers and provisions a device when it first connects to AWS IoT. This is a good option if you need to register large numbers of devices, but you don't have information about them that you can assemble into a bulk provisioning list.
- Bulk provisioning. This option allows you to specify a list of single-thing provisioning template values that are stored in a file in an S3 bucket. This approach works well if you have a large number of known devices whose desired characteristics you can assemble into a list.

Just-in-time provisioning and bulk provisioning are better options if you need to provision large numbers of devices. AWS IoT also provides a RegisterThing API that you can use to provision single devices programmatically.

Provisioning Templates

A provisioning template is a JSON document that uses parameters to describe the resources your device must use to interact with AWS IoT. A template contains two sections: Parameters and Resources.

Parameters Section

The Parameters section declares the parameters used in the Resources section. Each parameter declares a name, a type, and an optional default value. The default value is used when the dictionary
passed in with the template does not contain a value for the parameter. The Parameters section of a template document looks like the following:

```
"Parameters" : {
  "ThingName" : {
    "Type" : "String",
  },
  "SerialNumber" : {
    "Type" : "String",
  },
  "Location" : {
    "Type" : "String",
    "Default" : "WA"
  },
  "CSR" : {
    "Type" : "String",
  }
}
```

This template snippet declares four parameters: ThingName, SerialNumber, Location, and CSR. All of these parameters are of type String. The Location parameter declares a default value of "WA".

**Resources Section**

The Resources section of the template declares the resources required for your device to communicate with AWS IoT: a thing, a certificate, and one or more policies. Each resource specifies a logical name, a type, and a set of properties.

A logical name allows you to refer to a resource elsewhere in the template.

The type specifies the kind of resource you are declaring. Valid types are:

- AWS::IoT::Thing
- AWS::IoT::Certificate
- AWS::IoT::Policy

The properties you specify depend on the type of resource you are declaring.

**Thing Resources**

Thing resources are declared using the following properties:

- **ThingName**: String.
- **AttributePayload**: Optional. A list of name/value pairs.
- **ThingTypeName**: Optional. String for an associated thing type for the thing.
- **ThingGroups**: Optional. A list of groups to which the thing belongs.

**Certificate Resources**

Certificates can be specified in one of the following ways:

- A certificate signing request (CSR).
- A certificate ID of an existing device certificate.
- A device certificate created with a CA certificate registered with AWS IoT. If you have more than one CA certificate registered with the same subject field, you must also pass in the CA certificate used to sign the device certificate.
Note
When you declare a certificate in a template, use only one of these methods. For example, if you use a CSR, you cannot also specify a certificate ID or a device certificate.

For more information, see AWS IoT and Certificates.

Certificate resources are declared using the following properties:

- Status: Optional. String that can be one of: ACTIVE, INACTIVE, PENDING_ACTIVATION. Defaults to ACTIVE.

Examples:

- Certificate specified with a CSR:

```
"certificate" : {
    "Type" : "AWS::IoT::Certificate",
    "Properties" : {
        "CertificateSigningRequest": {"Ref" : "CSR"},
        "Status" : "ACTIVE"
    }
}
```

- Certificate specified with an existing certificate ID:

```
"certificate" : {
    "Type" : "AWS::IoT::Certificate",
    "Properties" : {
        "CertificateId": {"Ref" : "CertificateId"}
    }
}
```

- Certificate specified with an existing certificate .pem and CA certificate .pem:

```
"certificate" : {
    "Type" : "AWS::IoT::Certificate",
    "Properties" : {
        "CACertificatePem": {"Ref" : "CACertificatePem"},
    }
}
```

Policy Resources

Policy resources are declared using one the following properties:

- PolicyName: Optional. String. Defaults to a hash of the policy document.
- PolicyDocument: Optional. A JSON object specified as an escaped string. If PolicyDocument is not provided, the policy must already be created.

Note
If a Policy section is present, PolicyName or PolicyDocument, but not both, must be specified.
**Override Settings**

If a template specifies a resource that already exists, the **OverrideSettings** section allows you to specify the action to take:

**DO NOTHING**

Leave the resource as is.

**REPLACE**

Replace the resource with the resource specified in the template.

**FAIL**

Cause the request to fail with a **ResourceConflictsException**.

**MERGE**

Valid only for the **ThingGroups** and **AttributePayload** properties of a thing. Merge the existing attributes or group memberships of the thing with those specified in the template.

When you declare a thing resource, you can specify **OverrideSettings** for the following properties:

- **ATTRIBUTE_PAYLOAD**
- **THING_TYPE_NAME**
- **THING_GROUPS**

When you declare a certificate resource, you can specify **OverrideSettings** for the **Status** property.

**OverrideSettings** are not available for policy resources.

**Resource Example**

The following template snippet declares a thing, a certificate, and a policy:

```json
"Resources" : {
  "thing" : {
    "Type" : "AWS::IoT::Thing",
    "Properties" : {
      "ThingName" : {"Ref" : "ThingName"},
      "AttributePayload" : { "version" : "v1", "serialNumber" : {"Ref" : "SerialNumber"}},
      "ThingTypeName" : "lightBulb-versionA",
      "ThingGroups" : ["v1-lightbulbs", {"Ref" : "Location"}]
    },
    "OverrideSettings" : {
      "AttributePayload" : "MERGE",
      "ThingTypeName" : "REPLACE",
      "ThingGroups" : "DO NOTHING"
    }
  },
  "certificate" : {
    "Type" : "AWS::IoT::Certificate",
    "Properties" : {
      "CertificateSigningRequest" : {"Ref" : "CSR"},
      "Status" : "ACTIVE"
    },
    "OverrideSettings" : {
      "Status" : "DO NOTHING"
    }
  }
}``
The thing is declared with:

- The logical name "thing".
- The type AWS::IoT::Thing.
- A set of thing properties.

The thing properties include the thing name, a set of attributes, an optional thing type name, and an optional list of thing groups to which the thing belongs.

Parameters are referenced by "{Ref": "<parameter-name>"}. When the template is evaluated, the parameters are replaced with the parameter's value from the dictionary passed in with the template.

The certificate is declared with:

- The logical name "certificate".
- The type AWS::IoT::Certificate.
- A set of properties.

The properties include the CSR for the certificate, and setting the status to ACTIVE. The CSR text is passed as a parameter in the dictionary passed with the template.

The policy is declared with:

- The logical name "policy".
- The type AWS::IoT::Policy.
- Either the name of an existing policy or a policy document.

Template Example

The following JSON file is an example of a complete provisioning template that specifies the certificate with a CSR:

(The PolicyDocument field value must be a JSON object specified as an escaped string.)

```json
{
    "Parameters" : {
        "ThingName" : {
            "Type" : "String"
        },
        "SerialNumber" : {
            "Type" : "String"
        },
        "Location" : {
```

373
The following JSON file is an example of a complete provisioning template that specifies an existing certificate with a certificate ID:

```json
{
    "Parameters" : {
        "ThingName" : {
            "Type" : "String"
        },
        "SerialNumber" : {
            "Type" : "String"
        },
        "Location" : {
            "Type" : "String",
            "Default" : "WA"
        },
        "CSR" : {
            "Type" : "String"
        }
    },
    "Resources" : {
        "thing" : {
            "Type" : "AWS::IoT::Thing",
            "Properties" : {
                "ThingName" : {"Ref" : "ThingName"},
                "AttributePayload" : { "version" : "v1", "serialNumber" : {"Ref" : "SerialNumber"}},
                "ThingTypeName" : "lightBulb-versionA",
                "ThingGroups" : ["v1-lightbulbs", {"Ref" : "Location"}]
            }
        },
        "certificate" : {
            "Type" : "AWS::IoT::Certificate",
            "Properties" : {
                "CertificateSigningRequest" : {"Ref" : "CSR"},
                "Status" : "ACTIVE"
            }
        },
        "policy" : {
            "Type" : "AWS::IoT::Policy",
            "Properties" : {
            }
        }
    }
}
```
Programmatic Provisioning

To provision a thing, use the `RegisterThing` API or the `register-thing` CLI command. The `register-thing` CLI command takes the following arguments:

---template-body

The provisioning template.

---parameters

A list of name/value pairs for the parameters used in the provisioning template, in JSON format (for example, `{"ThingName" : "MyProvisionedThing", "CSR" : "<csr-text>"`).

See Provisioning Templates (p. 369).

RegisterThing or `register-thing` returns the ARNs for the resources and the text of the certificate it created:

```json
{
    "certificatePem": "<certificate-text>",
    "resourceArns": {
        "certificate": "arn:aws:iot:us-west-2:123456789012:cert/cd82bb924d4c6cbb14986dbb4f4030f3d892cc6b3c7ad5008ed542eaa2b049",
    }
}
```
Just-in-Time Provisioning

You can have your devices provisioned when they first attempt to connect to AWS IoT. Just-in-time provisioning (JITP) settings are made on CA certificates. To provision the device, you must enable automatic registration and associate a provisioning template with the CA certificate used to sign the device certificate.

You can make these settings when you register a CA certificate with the `RegisterCACertificate` API or the `register-ca-certificate` CLI command:

```bash
aws iot register-ca-certificate --ca-certificate <your-ca-cert> --verification-cert <your-verification-cert> --set-as-active --allow-auto-registration --registration-config file://<your-template>
```

For more information, see Registering a CA certificate.

You can also use the `UpdateCACertificate` API or the `update-ca-certificate` CLI command to update the settings for a CA certificate:

```bash
$ aws iot update-ca-certificate --cert-id <caCertificateId> --new-auto-registration-status ENABLE --registration-config file://<your-template>
```

When a device attempts to connect to AWS IoT by using a certificate signed by a registered CA certificate, AWS IoT loads the template from the CA certificate and calls `RegisterThing` using the template. The JITP workflow first registers a certificate with a status value of PENDING_ACTIVATION. When the device provisioning flow is complete, the status of the certificate is changed to ACTIVE.

AWS IoT defines the following parameters that you can declare and reference in provisioning templates:

- `AWS::IoT::Certificate::Country`
- `AWS::IoT::Certificate::Organization`
- `AWS::IoT::Certificate::OrganizationalUnit`
- `AWS::IoT::Certificate::DistinguishedNameQualifier`
- `AWS::IoT::Certificate::StateName`
- `AWS::IoT::Certificate::CommonName`
- `AWS::IoT::Certificate::SerialNumber`
- `AWS::IoT::Certificate::Id`

The values for these provisioning template parameters are limited to what JITP can extract from the subject field of the certificate of the device being provisioned.

The following JSON file is an example of a complete JITP template. The value of the `templateBody` field must be a JSON object specified as an escaped string and can use only the values in the preceding list. You can use a variety of tools to create the stringified JSON object, such as `json.dumps` (Python) or `JSON.stringify` (Node). The value of the `roleARN` field must be the ARN of a role that has the
AWSIoTThingsRegistration attached to it. Also, your template can use an existing PolicyName instead of the inline PolicyDocument in the example. (The first example adds line breaks for readability, but you can copy and paste the template that appears directly below it.)

```json
{
  "templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{
    "Parameters": {
      "AWS::IoT::Certificate::CommonName": {
        "Type": "String"
      },
      "AWS::IoT::Certificate::SerialNumber": {
        "Type": "String"
      },
      "AWS::IoT::Certificate::Country": {
        "Type": "String"
      },
      "AWS::IoT::Certificate::Id": {
        "Type": "String"
      }
    },
    "Resources": {
      "thing": {
        "Type": "AWS::IoT::Thing",
        "Properties": {
          "ThingName": {
            "Ref": "AWS::IoT::Certificate::CommonName"
          },
          "AttributePayload": {
            "version": "v1",
            "serialNumber": {
              "Ref": "AWS::IoT::Certificate::SerialNumber"
            }
          },
          "ThingTypeName": "lightBulb-versionA",
          "ThingGroups": [
            "v1-lightbulbs",
            {
              "Ref": "AWS::IoT::Certificate::Country"
            }
          ]
        },
        "OverrideSettings": {
          "AttributePayload": "MERGE",
          "ThingTypeName": "REPLACE",
          "ThingGroups": "DO_NOTHING"
        }
      },
      "certificate": {
        "Type": "AWS::IoT::Certificate",
        "Properties": {
          "CertificateId": {
            "Ref": "AWS::IoT::Certificate::Id"
          },
          "Status": "ACTIVE"
        },
        "OverrideSettings": {
          "Status": "DO_NOTHING"
        }
      },
      "policy": {
        "Type": "AWS::IoT::Policy",
        "Properties": {
          "PolicyDocument": "{
            "Version": "2012-10-17",
            "Statement": [{
              "Effect": "Allow",
              "Action": ["iot:Publish"]
            }]
          }
        }
      }
    },
    "roleArn": "arn:aws:iam::123456789012:role/Provisioning-JITP"
  }
}
```

Version you can copy and paste:

```json
{
  "templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{"templateBody": "{
    "Parameters": {
      "AWS::IoT::Certificate::CommonName": {
        "Type": "String"
      },
      "AWS::IoT::Certificate::SerialNumber": {
        "Type": "String"
      },
      "AWS::IoT::Certificate::Country": {
        "Type": "String"
      },
      "AWS::IoT::Certificate::Id": {
        "Type": "String"
      }
    },
    "Resources": {
      "thing": {
        "Type": "AWS::IoT::Thing",
        "Properties": {
          "ThingName": {
            "Ref": "AWS::IoT::Certificate::CommonName"
          },
          "AttributePayload": {
            "version": "v1",
            "serialNumber": {
              "Ref": "AWS::IoT::Certificate::SerialNumber"
            }
          },
          "ThingTypeName": "lightBulb-versionA",
          "ThingGroups": [
            "v1-lightbulbs",
            {
              "Ref": "AWS::IoT::Certificate::Country"
            }
          ]
        },
        "OverrideSettings": {
          "AttributePayload": "MERGE",
          "ThingTypeName": "REPLACE",
          "ThingGroups": "DO_NOTHING"
        }
      },
      "certificate": {
        "Type": "AWS::IoT::Certificate",
        "Properties": {
          "CertificateId": {
            "Ref": "AWS::IoT::Certificate::Id"
          },
          "Status": "ACTIVE"
        },
        "OverrideSettings": {
          "Status": "DO_NOTHING"
        }
      },
      "policy": {
        "Type": "AWS::IoT::Policy",
        "Properties": {
          "PolicyDocument": "{
            "Version": "2012-10-17",
            "Statement": [{
              "Effect": "Allow",
              "Action": ["iot:Publish"]
            }]
          }
        }
      }
    },
    "roleArn": "arn:aws:iam::123456789012:role/Provisioning-JITP"
  }
}
```

377
This sample template declares values for the AWS::IoT::Certificate::CommonName, AWS::IoT::Certificate::SerialNumber, AWS::IoT::Certificate::Country and AWS::IoT::Certificate::Id provisioning parameters that are extracted from the certificate and used in the Resources section. The JIPT workflow then uses this template to perform the following actions:

- Register a certificate and set its status to PENDING_ACTIVE.
- Create one thing resource.
- Create one policy resource.
- Attach the policy to the certificate.
- Attach the certificate to the thing.
- Update the certificate status to ACTIVE.

You should be able to see the certificate registration as a logged event (RegisterCACertificate) in AWS CloudTrail. You can also use CloudTrail to troubleshoot issues with your JIPT template.

### Bulk Provisioning

You can use the `start-thing-registration-task` command to provision things in bulk. This command takes a provisioning template, an Amazon S3 bucket name, a key name, and a role ARN that allows access to the file in the Amazon S3 bucket. The file in the Amazon S3 bucket contains the values used to replace the parameters in the template. The file must be a newline-delimited JSON file. Each line contains all of the parameter values for provisioning a single device. For example:

```json
{"ThingName": "foo", "SerialNumber": "123", "CSR": "csr1"}
```
The following bulk provisioning-related APIs might be useful:

- **ListThingRegistrationTasks** – Lists the current bulk thing provisioning tasks.
- **DescribeThingRegistrationTask** – Provides information about a specific bulk thing provisioning task.
- **StopThingRegistrationTask** – Stops a bulk thing provisioning task.
- **ListThingRegistrationTaskReports** – Used to check the results and/or failures for a bulk thing provisioning task.

**Note**
Only one bulk provisioning operation task can run at a time (per account).
Fleet Indexing Service

Fleet Indexing is a managed service that allows you to index and search your registry and shadow data in the cloud. After your fleet index is set up, the service manages the indexing of all your registry and shadow updates. You can use a simple query language to search across this data.

To get started, enable indexing and AWS IoT creates the index for your things. After it is active, you can run queries on your index. AWS IoT keeps it continuously updated with your latest data.

You can use the AWS IoT console to manage your indexing configuration and run your search queries. If you prefer programmatic access, you can use the AWS SDKs or the AWS CLI.

Please note that there are additional costs for using this service, beyond the standard charges for AWS IoT services, which are outlined in AWS IoT Device Management Pricing.

Managing Indexing

AWS_Things is the index created for all of your things. You can control whether you want to index only registry data or both registry and shadow data.

Enabling Indexing

You can create the AWS_Things index and control its configuration by using the thing-indexing-configuration setting in the UpdateIndexingConfiguration API. You can retrieve the current indexing configuration by using the GetIndexingConfiguration API.

The following command shows how to use the get-indexing-configuration CLI command to retrieve the current thing-indexing configuration:

```bash
aws iot get-indexing-configuration
{
   "thingIndexingConfiguration": {
      "thingIndexingMode": "OFF"
   }
}
```

You can use the AWS IoT update-indexing-configuration CLI command to update the thing-indexing configuration:

```bash
aws iot update-indexing-configuration --thing-indexing-configuration
thingIndexingMode=REGISTRY_AND_SHADOW
```

Valid values for thing-indexing-configuration are:

- **OFF**
  - No indexing/delete index.
- **REGISTRY**
  - Create or configure the AWS_Things index to index registry data only.
- **REGISTRY_AND_SHADOW**
  - Create or configure the AWS_Things index to index registry and shadow data.
Note
Normally, shadows are encrypted. However, if you decide to include shadows in the AWS_Things index, the data will be decrypted in order to index it.

Describing Indexes

The following command shows you how to use the describe-index CLI command to retrieve the current status of the index:

```bash
code
aws iot describe-index --index-name "AWS_Things"
{
    "indexName": "AWS_Things",
    "indexStatus": "BUILDING",
    "schema": "REGISTRY_AND_SHADOW"
}
```

The first time you enable indexing, AWS IoT builds your index. You cannot query the index if the indexStatus is BUILDING. The schema indicates which type of data, REGISTRY or REGISTRY_AND_SHADOW, is indexed.

Changing the configuration for your index causes the index to be rebuilt. The indexStatus during this process is REBUILDING. You can execute queries on the existing data while a rebuild is in progress. For example, if you change the index configuration from REGISTRY to REGISTRY_AND_SHADOW, while the index is being rebuilt, you can query registry data, including the latest updates, but you cannot query the shadow data until the rebuild is complete. The amount of time it takes to build or rebuild the index depends on the amount of data.

What is Indexed

Note the following restrictions and limitations:

Shadow fields with complex types:

A shadow field is indexed only if the value of the field is a simple type or an array consisting entirely of simple types. (By "simple type" we mean a string, a number, or one of the literals true or false). If a field's value is itself a JSON object, or an array containing an object, indexing will not be done on that field. For example, given shadow state:

```json
{
    "state": {
        "reported": {
            "switched": "ON",
            "colors": [ "RED", "GREEN", "BLUE" ],
            "palette": [ ]
        },
        "name": "RED",
        "intensity": 124
    },
    "name": "GREEN",
    "intensity": 68
},
"name": "BLUE",
"intensity": 201
}
```
the value of field "palette" will NOT be indexed since it is an array whose items are "objects". The value of field "colors" WILL be indexed since each value in the array is a string.

Shadow metadata:

A field in a shadow's metadata section is indexed, but only if the corresponding field in the the shadow's "state" section is indexed. (In the above example, the "palette" field in the shadow's metadata section will not be indexed either.)

Unregistered shadows:

If you create a shadow using a thing name which has not been registered in your AWS IoT account (using CreateThing), fields in this shadow will not be indexed.

Numeric values:

If any registry or shadow data which is being indexed is recognized by the service as a numeric value, it is indexed as such. You may form queries involving ranges and comparison operators on numeric values, for example "attribute.foo<5" or "shadow.reported.foo:[75 TO 80]". To be recognized as numeric, the value of the data must be a valid JSON "number" type literal (an integer in the range \(-2^{53}...2^{53}-1\), or a double-precision floating point with optional exponential notation) or part of an array containing only such values.

Null values:

Null values are not indexed.

Querying an Index

The following command shows how to use the search-index CLI command to query data in the index:

```
aws iot search-index --index-name "AWS_Things" --query-string "thingName:mything*"
```

```json
"things":[
    {"thingName":"mything1",
     "thingGroupNames": ["mygroup1"],
     "thingId":"a4b9f759-b0f2-4857-8a4b-967745ed9f4e",
     "attributes":{
       "attribute1":"abc"
     }
    },
    {"thingName":"mything2",
     "thingTypeName":"MyThingType",
     "thingGroupNames": ["mygroup1", "mygroup2"],
     "thingId":"01014ef9-e97e-44c6-985a-d0b06924f2af",
     "attributes":{
       "model":"1.2",
       "country":"usa"
     },
     "shadow":{
       "desired":{
         "location":"new york",
         "myvalues":[3, 4, 5]
       },
       "reported":{
```
Query Syntax

Queries are specified using a simple query syntax.

The query syntax supports the following features.

- Terms and phrases
- Searching fields
- Prefix search
- Range search
- Boolean operators AND, OR, NOT and –
- Grouping
- Field grouping
- Escaping special characters

The query syntax doesn't support the following features.

- Leading wildcard search (such as "*xyz"), but searching for "*" will match all things
- Regular expressions
- Boosting
- Ranking
- Fuzzy searches
• Proximity search
• Sorting
• Aggregation

A few things to note about the query language:

• The default operator is AND. A query for “thingName:abc thingType:xyz” is equivalent to “thingName:abc AND thingType:xyz”.
• If a field is not specified, AWS IoT searches for the term in all fields.
• All field names are case-sensitive.
• Search is case-insensitive. Words are separated by whitespace characters as defined by Java's Character.isWhitespace(int).
• Indexing of shadow data includes reported, desired, delta, and metadata sections.
• Shadow and registry versions are not searchable, but are present in the response.
• The maximum number of terms in a query is 5.

Example Queries

Queries are specified in a query string and passed to the SearchIndex API. The following table lists some example query strings:

<table>
<thead>
<tr>
<th>Query String</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>abc</td>
<td>Queries for &quot;abc&quot; in any registry or shadow field.</td>
</tr>
<tr>
<td>thingName:myThingName</td>
<td>Queries for a thing with name &quot;myThingName&quot;.</td>
</tr>
<tr>
<td>thingName:my*</td>
<td>Queries for things with names that begin with &quot;my&quot;.</td>
</tr>
<tr>
<td>thingName:ab?</td>
<td>Queries for things with names that have &quot;ab&quot; plus one additional character, for example: &quot;aba&quot;, &quot;abb&quot;, &quot;abc&quot; etc.</td>
</tr>
<tr>
<td>attributes.myAttribute:75</td>
<td>Queries for things with an attribute called &quot;MyAttribute&quot; that has the value 75.</td>
</tr>
<tr>
<td>attributes.myAttribute:[75 TO 80]</td>
<td>Queries for things with an attribute called &quot;MyAttribute&quot; whose value falls within a numeric range (75 - 80, inclusive).</td>
</tr>
<tr>
<td>attributes.myAttribute:[75 TO 80]</td>
<td>Queries for things with an attribute called &quot;MyAttribute&quot; whose value falls within the numeric range (&gt;75 and &lt;=80).</td>
</tr>
<tr>
<td>attributes.serialNumber:&quot;abcd&quot; TO &quot;abcf&quot;</td>
<td>Queries for things with an attribute called &quot;serialNumber&quot; whose value is within an alphanumeric string range. This query will return things with a &quot;serialNumber&quot; attribute with values &quot;abcd&quot;, &quot;abce&quot;, or &quot;abcf&quot;.</td>
</tr>
<tr>
<td>attributes.myAttribute:i*t</td>
<td>Queries for things with an attribute called &quot;MyAttribute&quot; whose value is 'i', followed by any number of characters, followed by 't'.</td>
</tr>
</tbody>
</table>
### Query String

<table>
<thead>
<tr>
<th>Query String</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>attributes.attr1:abc AND attributes.attr2&lt;5 NOT attributes.attr3&gt;10</td>
<td>Queries for things that combine terms using Boolean expressions. This query will return things that have an attribute named &quot;attr1&quot; with a value &quot;abc&quot;, an attribute named &quot;attr2&quot; that is less than 5, and an attribute named &quot;attr3&quot; that is not greater than 10.</td>
</tr>
<tr>
<td>shadow.hasDelta:true</td>
<td>Queries for things whose shadow has a delta element.</td>
</tr>
<tr>
<td>NOT attributes.model:legacy</td>
<td>Queries for things where the attribute model is not &quot;legacy&quot;.</td>
</tr>
</tbody>
</table>
| shadow.reported.stats.battery:(>70 AND <100) (v2 OR v3) NOT attributes.model:legacy | Queries for things with the following:  
  - The thing's shadow stats.battery attribute has a value between 70 and 100.  
  - The text "v2" or "v3" occurs in a thing's name, type name, or attribute values.  
  - The thing's model attribute is not set to "legacy". |
| shadow.reported.myvalues:2 | Queries for things where the myvalues array in the shadow's reported section contains a value of 2. |
| shadow.reported.location:* NOT shadow.desired.stats.battery:* | Queries for things with the following:  
  - The location attribute exists in the shadow's reported section.  
  - The stats.battery attribute does not exist in the shadow's desired section. |

### Authorization

You can specify the things index as a resource ARN in an AWS IoT policy action:

<table>
<thead>
<tr>
<th>Action</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>iot:SearchIndex</td>
<td>An index ARN (for example, arn:aws:iot:&lt;your-aws-region&gt;:index/AWS_Things).</td>
</tr>
<tr>
<td>iot:DescribeIndex</td>
<td>An index ARN (for example, arn:aws:iot:&lt;your-aws-region&gt;:index/AWS_Things).</td>
</tr>
</tbody>
</table>
Device Defender

AWS IoT Device Defender is an AWS IoT security service that allows you to audit the configuration of your devices, monitor connected devices to detect abnormal behavior, and to mitigate security risks. It gives you the ability to enforce consistent security policies across your AWS IoT device fleet and respond quickly when devices are compromised.

IoT fleets may consist of large numbers of devices that have diverse capabilities, are long-lived, and are geographically distributed. These characteristics make fleet setup complex and error-prone. And since devices are often constrained in computational power, memory, and storage capabilities, this limits the use of encryption and other forms of security on the devices themselves. Also, devices often use software with known vulnerabilities. The combination of these factors makes IoT fleets an attractive target for hackers and make it difficult to secure your device fleet on an ongoing basis.

Device Defender addresses these challenges by providing tools to identify security issues and deviations from best practices. Device Defender can audit device fleets to ensure they adhere to security best practices and detect abnormal behavior on devices.

Audit

Device Defender audits look at account and device-related settings and policies to ensure security measures are in place. An audit can help you detect any drifts from security best practices or proper access policies, such as multiple devices using the same identity, or overly-permissive policies that allow one device to read and update data for many other devices. You can run audits as needed (“on-demand audits”) or schedule them to be run periodically (“scheduled audits”).

A Device Defender audit runs a set of pre-defined checks (Audit checks (p. 386)) for common IoT security best practices and device vulnerabilities. Examples of pre-defined checks include policies that grant permission to read or update data on multiple device’s, devices that share an identity (X.509 certificate), or certificates that are expiring or have been revoked but are still active.

Audit checks

Note
When a check is enabled, data collection begins immediately. If you have a large amount of data in your account to be collected, then results of the check may not be available for some time after you have enabled it.

The following audit checks are supported:

REVOKECA_CERTCHECK

A CA certificate was revoked but is still active in AWS IoT.

Severity: Critical

A CA certificate is marked as revoked in the Certificate Revocation List maintained by the issuing authority, but is still marked as "ACTIVE" or "PENDING_TRANSFER" in the AWS IoT system.

The following reason codes are returned when this check finds a non-compliant CA certificate:

- CERTIFICATE_REVOKED_BY_ISSUER
why it matters (1)

A revoked CA certificate should no longer be used to sign device certificates. It may have been revoked because it was compromised, and newly added devices with certificates signed using this CA certificate might pose a security threat.

how to fix it (1)

1. Mark the CA certificate as "INACTIVE" in the AWS IoT system using UpdateCACertificate.
2. Review the device certificate registration activity for the time after the CA certificate was revoked and consider revoking any device certificates that may have been issued with it during this time. (Use ListCertificatesByCA to list the device certificates signed by the CA certificate and UpdateCertificate to revoke a device certificate.)

DEVICE_CERTIFICATE_SHARED_CHECK

Multiple, concurrent connections use the same X.509 certificate to authenticate with the AWS IoT service.

Severity: Critical

more info (2)

When this check is enabled, data collection begins immediately, but results of the check are not available for at least two hours.

When performed as part of an on-demand audit, this check looks at the certificates and client IDs that were used by devices to connect during the 31 days prior to the start of the audit. For scheduled audits, this check looks at data from the last time the audit was run to the time this instance of the audit started. If you have taken steps to mitigate this condition during the time checked, note when the concurrent connections were made to determine if the problem persists.

The following reason codes are returned when this check finds a non-compliant certificate:

• CERTIFICATE_SHARED_BY_MULTIPLE_DEVICES

In addition, the findings returned by this check include the ID of the shared certificate, the IDs of the clients using the certificate to connect, and the connect/disconnect times. Results are listed in order of most recent first.

why it matters (2)

Each device should have a unique certificate to authenticate with AWS IoT. When multiple devices use the same certificate this may indicate that a device has been compromised and its identity cloned in order to further compromise the system.

how to fix it (2)

Verify that the device certificate has not been compromised. If it has, follow your security best practices to mitigate the situation.

If you are using the same certificate on multiple devices, you may want to:

1. Provision new, unique certificates and attach them to each device.
2. Verify that the new certificates are valid and the devices are able to use them to connect.
3. Mark the old certificate as "REVOKED" in the AWS IoT system using UpdateCertificate.
4. Detach the old certificate from each of the devices.
UNAUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK

A policy attached to an unauthenticated Cognito identity pool role is considered overly-permissive because it grants permission to perform any of the following AWS IoT actions:

- manage or modify things
- read thing administrative data
- manage non-thing related data or resources

Or, because it grants permission to perform the following AWS IoT actions on a broad set of devices:

- use MQTT to connect/publish/subscribe to reserved topics (including shadow or job execution data)
- use API commands to read or modify shadow or job execution data

In general, devices which connect using an unauthenticated Cognito identity pool role should have only limited permission to publish/subscribe to thing-specific MQTT topics or use the API commands to read/modify thing-specific data related to shadow or job execution data.

Severity: **Critical**

**manage or modify things** (3)

The following AWS IoT API actions are used to manage or modify things so permission to perform these should not be granted to devices connecting via an unauthenticated Cognito identity pool:

- AddThingToThingGroup
- AttachThingPrincipal
- CreateThing
- DeleteThing
- DetachThingPrincipal
- ListThings
- ListThingsInThingGroup
- RegisterThing
- RemoveThingFromThingGroup
- UpdateThing
- UpdateThingGroupsForThing

Any role that grants permission to perform these actions on even a single resource is considered non-compliant.

**read thing administrative data** (3)

The following AWS IoT API actions are used to read or modify thing data so devices connecting via an unauthenticated Cognito identity pool should not be given permission to perform these:

- DescribeThing
- ListJobExecutionsForThing
- ListThingGroupsForThing
- ListThingPrincipals

**Example:**

- non-compliant:
Audit checks

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:DescribeThing",
        "iot:ListJobExecutionsForThing",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals"
      ],
      "Resource": [
        "arn:aws:iot:<region>:<account-id>:/thing/MyThing"
      ]
    }
  ]
}
```

This allows the device to perform the specified actions even though it is granted for only one specific thing.

manage non-things (3)

Devices connecting via an unauthenticated Cognito identity pool should not be given permission to perform any other AWS IoT API actions other than those discussed in these sections. In order to manage your account with an application that connects via an unauthenticated Cognito identity pool, create a separate identity pool not used by devices.

subscribe/publish to MQTT topics (3)

MQTT messages are sent through the AWS IoT Message Broker and are used by devices to perform many different actions, including accessing and modifying shadow state and job execution state. A policy that grants permission to a device to connect, publish or subscribe to MQTT messages should restrict these actions to specific resources as follows:

Connect
- non-compliant:

  ```text
  arn:aws:iot:<region>:<account-id>:client/*
  ```

  The wildcard * allows any device to connect to AWS IoT.

  ```text
  arn:aws:iot:<region>:<account-id>:client/${iot:ClientId}
  ```

  Unless "iot:Connection.Thing.IsAttached" is set to true in the condition keys, this is equivalent to the wildcard * as in the previous example.

- compliant:

  ```json
  {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [ "iot:Connect" ],
      }
    ]
  }
  ```
The resource specification contains a variable that matches the device name used to connect, and the condition statement further restricts the permission by checking that the certificate used by the MQTT client matches that attached to the thing with the name used.

**Publish**

- non-compliant:

  ```
  ```

  This allows the device to update the shadow of any device (* = all devices).

- compliant:

  ```
  ```

  The resource specification contains a wildcard, but it only matches any shadow-related topic for the device whose thing name is used to connect.

**Subscribe**

- non-compliant:

  ```
  arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/*
  ```

  This allows the device to subscribe to reserved shadow or job topics for all devices.

- compliant:

  ```
  arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/*
  ```

  This allows the device to see shadow updates on any device (+ = all devices).
The resource specifications contain wildcards but they only match any shadow-related topic and any job-related topic for the device whose thing name is used to connect.

Receive

- compliant:

  `arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/*`

  This is okay because the device can only receive messages from topics on which it has permission to subscribe.

read/modify shadow or job data (3)

A policy that grants permission to a device to perform an API action to access or modify thing shadows or job execution data should restrict these actions to specific resources. The API actions are:

- DeleteThingShadow
- GetThingShadow
- UpdateThingShadow
- DescribeJobExecutions
- GetPendingJobExecutions
- StartNextPendingJobExecution
- UpdateJobExecution

Examples:

- non-compliant:

  `arn:aws:iot:<region>:<account-id>:thing/*`

  This allows the device to perform the specified action on any thing.

- compliant:

  ```json
  {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "iot:Subscribe" ],
      "Resource": [
      ]
    }
  ]
```
"Action": [
  "iot:DeleteThingShadow",
  "iot:GetThingShadow",
  "iot:UpdateThingShadow",
  "iot:DescribeJobExecution",
  "iot:GetPendingJobExecutions",
  "iot:StartNextPendingJobExecution",
  "iot:UpdateJobExecution"
],
"Resource": [
  "arn:aws:iot:<region>:<account-id>:/thing/MyThing1",
  "arn:aws:iot:<region>:<account-id>:/thing/MyThing2"
]
}
}

This allows the device to perform the specified actions on only two specific things.

more info (3)

For this check, Device Defender audits all Cognito identity pools that have been used to connect to the AWS IoT message broker during the past 31 days prior to the audit execution. All Cognito identity pools from which either an authenticated or unauthenticated Cognito identity connected are included in the audit.

The following reason codes are returned when this check finds a non-compliant unauthenticated Cognito identity pool role:

- ALLOWS_ACCESS_TO_IOT_ADMIN_ACTIONS
- ALLOWS_BROAD_ACCESS_TO_IOT_DATA_PLANE_ACTIONS

why it matters (3)

Because unauthenticated identities are never authenticated by the user, they pose a much greater risk than authenticated Cognito identities. If an unauthenticated identity is compromised it could use administrative actions to modify account settings, delete resources or gain access to sensitive data. Or, with broad access to device settings, it could access or modify shadows and jobs for all devices in your account. A guest user might use the permissions to compromise your entire fleet or launch a DDOS attack with messages.

how to fix it (3)

A policy attached to an unauthenticated Cognito identity pool role should grant only those permissions required for a device to do its job. We recommend the following steps:

1. Create a new compliant role.
2. Create a new Cognito identity pool and attach the compliant role to it.
3. Verify that your identities can access AWS IoT using the new pool.
4. Once verification is complete, attach the new, compliant role to the Cognito identity pool that was flagged as non-compliant.

AUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK

A policy attached to an authenticated Cognito identity pool role is considered overly-permissive because it grants permission to perform the following AWS IoT actions:
- manage or modify things
- manage non-thing related data or resources

Or, because it grants permission to perform the following AWS IoT actions on a broad set of devices:

- read thing administrative data
- use MQTT to connect/publish/subscribe to reserved topics (including shadow or job execution data)
- use API commands to read or modify shadow or job execution data

In general, devices that connect using an authenticated Cognito identity pool role should have only limited permission to read thing-specific administrative data, publish/subscribe to thing-specific MQTT topics or use the API commands to read/modify thing-specific data related to shadow or job execution data.

Severity: Critical

manage or modify things (4)

The following AWS IoT API actions are used to manage or modify things so permission to perform these should not be granted to devices connecting via an authenticated Cognito identity pool:

- AddThingToThingGroup
- AttachThingPrincipal
- CreateThing
- DeleteThing
- DetachThingPrincipal
- ListThings
- ListThingsInThingGroup
- RegisterThing
- RemoveThingFromThingGroup
- UpdateThing
- UpdateThingGroupsForThing

Any role that grants permission to perform these actions on even a single resource is considered non-compliant.

manage non-things (4)

Devices connecting via an authenticated Cognito identity pool should not be given permission to perform any other AWS IoT API actions other than those discussed in these sections. In order to manage your account with an application that connects via an authenticated Cognito identity pool, create a separate identity pool not used by devices.

read thing administrative data (4)

The following AWS IoT API actions are used to read thing data so devices connecting via an authenticated Cognito identity pool should be given permission to perform these on only a limited set of things:

- DescribeThing
- ListJobExecutionsForThing
- ListThingGroupsForThing
• ListThingPrincipals

Examples:

• non-compliant:

arn:aws:iot:<region>:<account-id>:thing/*

This allows the device to perform the specified action on any thing.

• compliant:

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:DescribeThing",
        "iot:ListJobExecutionsForThing",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals"
      ],
      "Resource": [
        "arn:aws:iot:<region>:<account-id>:/thing/MyThing" ]
    }
  ]
}

This allows the device to perform the specified actions on only one specific thing.

• compliant:

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:DescribeThing",
        "iot:ListJobExecutionsForThing",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals"
      ],
      "Resource": [
        "arn:aws:iot:<region>:<account-id>:/thing/MyThing*"
      ]
    }
  ]
}

This is compliant because, although the resource is specified with a wildcard (*), this is preceded by a specific string, and that limits the set of things accessed to those with names that have the given prefix.

subscribe/publish to MQTT topics (4)

MQTT messages are sent through the AWS IoT Message Broker and are used by devices to perform many different actions, including accessing and modifying shadow state and job execution state. A
policy that grants permission to a device to connect, publish or subscribe to MQTT messages should restrict these actions to specific resources as follows:

Connect

- non-compliant:

  ```
  arn:aws:iot:<region>:<account-id>:client/*
  ```

  The wildcard * allows any device to connect to AWS IoT.

  ```
  arn:aws:iot:<region>:<account-id>:client/${iot:ClientId}
  ```

  Unless "iot:Connection.Thing.IsAttached" is set to true in the condition keys, this is equivalent to the wildcard * as in the previous example.

- compliant:

  ```
  {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [ "iot:Connect" ],
        "Resource": [
        ],
        "Condition": {
          "Bool": { "iot:Connection.Thing.IsAttached": "true" }
        }
      }
    ]
  }
  ```

  The resource specification contains a variable that matches the device name used to connect, and the condition statement further restricts the permission by checking that the certificate used by the MQTT client matches that attached to the thing with the name used.

Publish

- non-compliant:

  ```
  ```

  This allows the device to update the shadow of any device (* = all devices).

  ```
  ```

  This allows the device to read/update/delete the shadow of any device.

- compliant:

  ```
  {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [ "iot:Publish" ],
        "Resource": [
        ```
The resource specification contains a wildcard, but it only matches any shadow-related topic for the device whose thing name is used to connect.

Subscribe

- non-compliant:

```
arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/*
```

This allows the device to subscribe to reserved shadow or job topics for all devices.

```
```

The same as the previous example, but using the # wildcard.

```
```

This allows the device to see shadow updates on any device (+ = all devices).

- compliant:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "iot:Subscribe" ],
      "Resource": [
        ${iot:Connection.Thing.ThingName}/shadow/**",
        ${iot:Connection.Thing.ThingName}/jobs/**",
        ${iot:Connection.Thing.ThingName}/shadow/*",
        ${iot:Connection.Thing.ThingName}/jobs/*"
      ]
    }
  ]
}
```

The resource specifications contain wildcards but they only match any shadow-related topic and any job-related topic for the device whose thing name is used to connect.

Receive

- compliant:

```
arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/*
```

This is okay because the device can only receive messages from topics on which it has permission to subscribe.
read/modify shadow or job data (4)

A policy that grants permission to a device to perform an API action to access or modify thing shadows or job execution data should restrict these actions to specific resources. The API actions are:

- DeleteThingShadow
- GetThingShadow
- UpdateThingShadow
- DescribeJobExecutions
- GetPendingJobExecutions
- StartNextPendingJobExecution
- UpdateJobExecution

**Examples:**

- **non-compliant:**

```
arn:aws:iot:<region>:<account-id>:thing/*
```

This allows the device to perform the specified action on any thing.

- **compliant:**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:DeleteThingShadow",
                "iot:GetThingShadow",
                "iot:UpdateThingShadow",
                "iot:DescribeJobExecution",
                "iot:GetPendingJobExecutions",
                "iot:StartNextPendingJobExecution",
                "iot:UpdateJobExecution"
            ],
            "Resource": [
                "arn:aws:iot:<region>:<account-id>:thing/MyThing1",
                "arn:aws:iot:<region>:<account-id>:thing/MyThing2"
            ]
        }
    ]
}
```

This allows the device to perform the specified actions on only two specific things.

more info (4)

For this check, Device Defender audits all Cognito identity pools that have been used to connect to the AWS IoT message broker during the past 31 days prior to the audit execution. All Cognito identity pools from which either an authenticated or unauthenticated Cognito identity connected are included in the audit.

The following reason codes are returned when this check finds a non-compliant authenticated Cognito identity pool role:

- ALLOWS_BROAD_ACCESS_TO_IOT_THING_ADMIN_READ_ACTIONS
• ALLOWS_ACCESS_TO_IOT_NON_THING_ADMIN_ACTIONS
• ALLOWS_ACCESS_TO_IOT_THING_ADMIN_WRITE_ACTIONS

why it matters (4)

If an authenticated identity is compromised it could use administrative actions to modify account settings, delete resources or gain access to sensitive data.

how to fix it (4)

A policy attached to an authenticated Cognito identity pool role should grant only those permissions required for a device to do its job. We recommend the following steps:

1. Create a new compliant role.
2. Create a new Cognito identity pool and attach the compliant role to it.
3. Verify that your identities can access AWS IoT using the new pool.
4. Once verification is complete, attach the new, compliant role to the Cognito identity pool that was flagged as non-compliant.

IOT_POLICY_OVERLY_PERMISSIVE_CHECK

An AWS IoT policy gives permissions that are too broad/unrestricted. It grants permission to send or receive MQTT messages for a broad set of devices, or grants permission to access or modify shadow and job execution data for a broad set of devices.

In general, a policy for a device should grant access to very specific resources associated with just that device and no, or very few, other devices. With certain exceptions, using a wildcard (for example, ") to specify resources in such a policy is considered too broad/unrestricted.

Severity: Critical

MQTT permissions (5)

MQTT messages are sent through the AWS IoT Message Broker and are used by devices to perform many different actions, including accessing and modifying shadow state and job execution state. A policy that grants permission to a device to connect, publish or subscribe to MQTT messages should restrict these actions to specific resources as follows:

Connect

• non-compliant:

```
arn:aws:iot:<region>:<account-id>:client/*
```

The wildcard * allows any device to connect to AWS IoT.

```
arn:aws:iot:<region>:<account-id>:client/#{iot:ClientId}
```

Unless "iot:Connection.Thing.IsAttached" is set to true in the condition keys, this is equivalent to the wildcard * as in the previous example.

• compliant:

```
{
  "Version": "2012-10-17",
```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": [ "iot:Connect" ],  
    "Resource": [  
    ],  
    "Condition": {  
      "Bool": { "iot:Connection.Thing.IsAttached": "true" }  
    }  
  }  
]

The resource specification contains a variable that matches the device name used to connect, and the condition statement further restricts the permission by checking that the certificate used by the MQTT client matches that attached to the thing with the name used.

Publish

• non-compliant:

```
```

This allows the device to update the shadow of any device (* = all devices).

```
```

This allows the device to read/update/delete the shadow of any device.

• compliant:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {  
      "Effect": "Allow",  
      "Action": [ "iot:Publish" ],  
      "Resource": [  
      ]
    }
  ]
}
```

The resource specification contains a wildcard, but it only matches any shadow-related topic for the device whose thing name is used to connect.

Subscribe

• non-compliant:

```
arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/*
```

This allows the device to subscribe to reserved shadow or job topics for all devices.

```
arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/*
```

The same as the previous example, but using the # wildcard.
Audit checks

```plaintext
```

This allows the device to see shadow updates on any device (+ = all devices).

- compliant:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "iot:Subscribe" ],
      "Resource": [
      ],
    }
  ]
}
```

The resource specifications contain wildcards but they only match any shadow-related topic and any job-related topic for the device whose thing name is used to connect.

Receive

- compliant:

```plaintext
arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/*
```

This is okay because the device can only receive messages from topics on which it has permission to subscribe.

shadow and job permissions (5)

A policy that grants permission to a device to perform an API action to access or modify thing shadows or job execution data should restrict these actions to specific resources. The API actions are:

- DeleteThingShadow
- GetThingShadow
- UpdateThingShadow
- DescribeJobExecutions
- GetPendingJobExecutions
- StartNextPendingJobExecution
- UpdateJobExecution

Examples:

- non-compliant:

```plaintext
arn:aws:iot:<region>:<account-id>:thing/*
```

This allows the device to perform the specified action on any thing.

- compliant:
This allows the device to perform the specified actions on only two specific things.

more info (5)

The following reason code is returned when this check finds a non-compliant IoT policy:

- ALLOWS_BROAD_ACCESS_TO_IOT_DATA_PLANE_ACTIONS

why it matters (5)

A certificate, Cognito identity or thing group with an overly-permissive policy can, if compromised, impact the security of your entire account. An attacker could use such broad access to read or modify shadows, jobs or job executions for all your devices. Or an attacker could use a compromised certificate to connect malicious devices or launch a DDOS attack on your network.

how to fix it (5)

Follow these steps to fix any non-compliant policies attached to things, thing groups, or other entities:

1. Create a new, compliant version of the policy using CreatePolicyVersion with the "setAsDefault" flag set to true (making this new version operative for all entities that use the policy).
2. Get a list of targets (certificates, thing groups) that the policy is attached to using ListTargetsForPolicy and determine which devices are included in the groups or which use the certificates to connect.
3. Verify that all associated devices are able to connect to AWS IoT. If a device is unable to connect, roll back the default policy to the previous version using SetPolicyVersion, revise the policy and try again.

Use AWS IoT Policy Variables to dynamically reference specific AWS IoT resources in your policies.
CA_CERT_APPROACHING_EXPIRATION_CHECK

A CA certificate is expiring within 30 days or has expired.

Severity: Medium

more info (6)

This check applies to CA certificates that are "ACTIVE" or "PENDING_TRANSFER".

The following reason codes are returned when this check finds a non-compliant CA certificate:

- CERTIFICATE_APPROACHING_EXPIRATION
- CERTIFICATE_PAST_EXPIRATION

why it matters (6)

An expired CA certificate should not be used to sign new device certificates.

how to fix it (6)

Consult your security best practices for how to proceed. You may want to:

1. Register a new CA certificate with AWS IoT.
2. Verify that you are able to sign device certificates using the new CA certificate.
3. Mark the old CA certificate as "INACTIVE" in the AWS IoT system using UpdateCACertificate.

CONFLICTING_CLIENT_IDS_CHECK

Multiple devices connect using the same client ID.

Severity: High

more info (7)

Multiple connections were made using the same client ID, causing an already connected device to be disconnected. The MQTT specification allows only one active connection per client ID, so when another device connects using the same client ID, it knocks the previous one off the connection.

When performed as part of an on-demand audit, this check looks at how clientIDs were used to connect during the 31 days prior to the start of the audit. For scheduled audits, this check looks at data from the last time the audit was run to the time this instance of the audit started. If you have taken steps to mitigate this condition during the time checked, note when the connections/disconnections were made to determine if the problem persists.

The following reason codes are returned when this check finds non-compliance:

- DUPLICATE_CLIENT_ID_ACROSS_CONNECTIONS

In addition, the findings returned by this check include the clientID used to connect, principal IDs, and disconnect times. Results are listed in order of most recent first.

why it matters (7)

Devices with conflicting IDs are forced to constantly reconnect, which may result in lost messages or leave a device unable to connect.

This may indicate that a device or a device's credentials have been compromised, and might be part of a DDoS attack. It is also possible that devices are misconfigured in the account or a device has a bad connection and is forced to reconnect several times per minute.
how to fix it (7)

Register each device as a unique thing in AWS IoT, and use the thing name as the client ID to connect. Or use a UUID as the client ID when connecting the device over MQTT.

DEVICE_CERT_APPROACHING_EXPIRATION_CHECK

A device certificate is expiring within 30 days or has expired.

Severity: Medium

This check applies to device certificates that are "ACTIVE" or "PENDING_TRANSFER".

The following reason codes are returned when this check finds a non-compliant device certificate:

- CERTIFICATE_APPROACHING_EXPIRATION
- CERTIFICATE_PAST_EXPIRATION

why it matters (8)

A device certificate should not be used after it expires.

how to fix it (8)

Consult your security best practices for how to proceed. You may want to:

1. Provision a new certificate and attach it to the device.
2. Verify that the new certificate is valid and the device is able to use it to connect.
3. Mark the old certificate as "INACTIVE" in the AWS IoT system using UpdateCertificate.
4. Detach the old certificate from the device. (See DetachThingPrincipal.)

REVOKED_DEVICE_CERT_CHECK

A revoked device certificate is still active.

Severity: Medium

A device certificate is in its CA's Certificate revocation list but it is still active in AWS IoT.

This check applies to device certificates that are "ACTIVE" or "PENDING_TRANSFER".

The following reason codes are returned when this check finds non-compliance:

- CERTIFICATE_REVOKED_BY_ISSUER

why it matters (9)

A device certificate is usually revoked because it has been compromised. It is possible that it has not yet been revoked in AWS IoT due to an error or an oversight.

how to fix it (9)

Verify that the device certificate has not been compromised. If it has, follow your security best practices to mitigate the situation. You may want to:
How To Perform Audits

1. Configure audit settings for your account. Use UpdateAccountAuditConfiguration (p. 411) to enable those checks you want to be available for audits, set up optional notifications, and configure permissions.

   For certain checks, AWS IoT begins collecting data as soon as the check is enabled.

2. Create one or more audit schedules. Use CreateScheduledAudit (p. 419) to specify the checks you want to perform during an audit and how often these audits should be run.

   Or, you can run an on-demand audit when necessary. Use StartOnDemandAuditTask (p. 436) to specify the checks you want to perform and start an audit running right away. (Results may not be ready for some time if you have recently enabled a check that is included in the on-demand audit.)

3. You can use the AWS IoT console to view the results of your audits.

   Or, you can see the results of your audits with ListAuditFindings (p. 449). With this command, you can filter the results by the type of check, a specific resource, or the time of the audit. Armed with this information, you can take the appropriate steps to mitigate any problems found.

Notifications

When an audit is completed, an SNS notification can be sent with a summary of the results of each audit check that was performed, including details about the number of non-compliant resources that were found. Use the auditNotificationTargetConfigurations field in the input to the UpdateAccountAuditConfiguration (p. 411) command. The SNS notification has the following payload:
payload example

```json
{
    "accountId": "123456789012",
    "taskId": "4e2bcd1ccbc2a5dd15292a82ab80c380",
    "taskStatus": "FAILED|CANCELED|COMPLETED",
    "taskType": "ON_DEMAND_AUDIT_TASK|SCHEDULED_AUDIT_TASK",
    "scheduledAuditName": "myWeeklyAudit",
    "failedChecksCount": 0,
    "canceledChecksCount": 0,
    "nonCompliantChecksCount": 1,
    "compliantChecksCount": 0,
    "totalChecksCount": 1,
    "taskStartTime": 1524740766191,
    "auditDetails": [
        {
            "checkName": "DEVICE_CERT_APPROACHING_EXPIRATION_CHECK | REVOKED_DEVICE_CERT_CHECK | CA_CERT_APPROACHING_EXPIRATION_CHECK | REVOKED_CA_CERT_CHECK | DEVICE_CERTIFICATE_SHARED_CHECK | IOT_POLICY_UNRESTRICTED_CHECK | UNAUTHENTICATED_COGNITO.IDENTITY.UNRESTRICTED_ACCESS_CHECK | AUTHENTICATED_COGNITO.IDENTITY.UNRESTRICTED_ACCESS_CHECK | CONFLICTING_CLIENT_IDS_CHECK | LOGGING_DISABLED_CHECK",
            "checkRunStatus": "FAILED | CANCELED | COMPLETED_COMPLIANT | COMPLETED_NON_COMPLIANT",
            "nonCompliantResourcesCount": 1,
            "totalResourcesCount": 1,
            "message": "optional message if an error occurred",
            "errorCode": "INSUFFICIENT_PERMISSIONS|AUDIT_CHECK_DISABLED"
        }
    ]
}
```

payload JSON schema

```json
{
    "$schema": "http://json-schema.org/draft-07/schema#",
    "$id": "arn:aws:iot:::schema:auditnotification/1.0",
    "type": "object",
    "properties": {
        "accountId": {
            "type": "string"
        },
        "taskId": {
            "type": "string"
        },
        "taskStatus": {
            "type": "string",
            "enum": ["FAILED", "CANCELED", "COMPLETED"]
        },
        "taskType": {
```
"type": "string",
"enum": [
  "SCHEDULED_AUDIT_TASK",
  "ON_DEMAND_AUDIT_TASK"
],
"scheduledAuditName": {
  "type": "string"
},
"failedChecksCount": {
  "type": "integer"
},
"canceledChecksCount": {
  "type": "integer"
},
"nonCompliantChecksCount": {
  "type": "integer"
},
"compliantChecksCount": {
  "type": "integer"
},
"totalChecksCount": {
  "type": "integer"
},
"taskStartTime": {
  "type": "integer"
},
"auditDetails": {
  "type": "array",
  "items": [
    {
      "type": "object",
      "properties": {
        "checkName": {
          "type": "string",
          "enum": [
            "DEVICE_CERT_APPROACHING_EXPIRATION_CHECK",
            "REVOKED_DEVICE_CERT_CHECK",
            "CA_CERT_APPROACHING_EXPIRATION_CHECK",
            "REVOKED_CA_CERT_CHECK",
            "LOGGING_DISABLED_CHECK"
          ]
        },
        "checkRunStatus": {
          "type": "string",
          "enum": [
            "FAILED",
            "CANCELED",
            "COMPLETED_COMPLIANT",
            "COMPLETED_NON_COMPLIANT"
          ]
        },
        "nonCompliantResourcesCount": {
          "type": "integer"
        },
        "totalResourcesCount": {
          "type": "integer"
        },
        "message": {
          "type": "string"
        },
        "errorCode": {
          "type": "string",
          "enum": [
            "INSUFFICIENT_PERMISSIONS",
            "AUDIT_CHECK_DISABLED"
          ]
        }
      }
    }
  ]
}
Notifications can also be viewed in the AWS IoT console, along with additional information about the device, device statistics (for example, last connection time, number of active connections, data transfer rate), and historical alerts for the device.

Permissions

This section contains information on how to set up the AWS IAM roles and policies required to create, run and manage Device Defender audits. For more information on AWS IAM, see the AWS Identity and Access Management User Guide.

Give Device Defender permission to collect your data in order to run an audit.

When you call UpdateAccountAuditConfiguration (p. 411) you must specify an IAM Role with two policies, a permissions policy and a trust policy. The permissions policy grants Device Defender permission to access your account data, using AWS IoT APIs, when it runs an audit. The trust policy grants Device Defender permission to assume the required role.

permissions policy

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "iot:GetLoggingOptions",
        "iot:GetV2LoggingOptions",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:DescribeCACertificate",
        "iot:ListCertificates",
        "iot:DescribeCA_certificate"
      ]
    }
  ]
}
```
Give Device Defender permission to publish notifications to an SNS topic.

If you use the `auditNotificationTargetConfigurations` parameter in `UpdateAccountAuditConfiguration (p. 411)`, you must specify an IAM Role with two policies, a permissions policy and a trust policy. The permissions policy grants permission to Device Defender to publish notifications to your SNS topic. The trust policy grants Device Defender permission to assume the required role.

**permissions policy**

```json

{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "sns:Publish"  
      ],  
      "Resource": [  
        "arn:aws:sns:region:account-id:your-topic-name"  
      ]  
    }  
  ]
}
```

**trust policy**

```json

{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "",  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "iot.amazonaws.com"  
      },  
      "Action": "sts:AssumeRole"  
    }  
  ]
}
```
trust policy

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "iot.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Give IAM users or groups permission to run Device Defender audit commands

To allow IAM users or groups to manage, run, or view the results of Device Defender audits, you must create and assign roles with attached policies that grant permission to run the appropriate commands. What each specific policy contains depends on what commands you want the user or group to run.

- **UpdateAccountAuditConfiguration**

policy

NOTE: You must create the IAM Role with the attached policy in same account from which this command is run. Cross account access is not allowed. The policy should have "iam:PassRole" permissions (permissions to pass this role).

In the following policy template `audit-permissions-role-arn` is the roleArn that you pass to Device Defender in the `UpdateAccountAuditConfiguration` request using the `roleArn` parameter. `audit-notifications-permissions-role-arn` is the roleArn that you pass to Device Defender in the `UpdateAccountAuditConfiguration` request using the `auditNotificationTargetConfigurations` parameter.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:UpdateAccountAuditConfiguration"
      ],
      "Resource": [
        "*
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": [
        "arn:aws:iam::account-id:role/audit-permissions-role-arn",
        "arn:aws:iam::account-id:role/audit-notifications-permissions-role-arn"
      ]
    }
  ]
}
```
• DescribeAccountAuditConfiguration
• DeleteAccountAuditConfiguration
• StartOnDemandAuditTask
• CancelAuditTask
• DescribeAuditTask
• ListAuditTasks
• ListScheduledAudits
• ListAuditFindings

NOTE: all these commands require * in the Resource field of the policy.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:DescribeAccountAuditConfiguration",
        "iot:DeleteAccountAuditConfiguration",
        "iot:StartOnDemandAuditTask",
        "iot:CancelAuditTask",
        "iot:DescribeAuditTask",
        "iot:ListAuditTasks",
        "iot:ListScheduledAudits",
        "iot:ListAuditFindings"
      ],
      "Resource": [
        "*
      ]
    }
  ]
}
```

• CreateScheduledAudit
• UpdateScheduledAudit
• DeleteScheduledAudit
• DescribeScheduledAudit

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:CreateScheduledAudit",
        "iot:UpdateScheduledAudit",
        "iot:DeleteScheduledAudit",
        "iot:DescribeScheduledAudit"
      ],
      "Resource": [
```
The format for a Device Defender scheduled audit roleArn is:

```
arn:aws:iot:region:account-id:scheduledaudit/scheduled-audit-name
```

## Service Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Limit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduled audits</td>
<td>5 max.</td>
<td>You can create up to 5 scheduled audits before a LimitExceeded Exception occurs.</td>
</tr>
<tr>
<td>simultaneous in progress &quot;on-demand&quot; audits</td>
<td>10 max.</td>
<td>You can create up to 10 &quot;on-demand&quot; audits before a LimitExceeded Exception occurs.</td>
</tr>
</tbody>
</table>

## Audit Commands

### Manage Audit Settings

Configure audit settings for your account using `UpdateAccountAuditConfiguration`. This command allows you to enable those checks you want to be available for audits, set up optional notifications, and configure permissions.

Check these settings with `DescribeAccountAuditConfiguration`.

Use `DeleteAccountAuditConfiguration` to delete your audit settings. This restores all default values, and effectively disables audits since all checks are disabled by default.

### UpdateAccountAuditConfiguration

Configures or reconfigures the Device Defender audit settings for this account. Settings include how audit notifications are sent and which audit checks are enabled or disabled.

**https**

**Request syntax:**

```
PATCH /audit/configuration
Content-type: application/json
```

```json
{
  "roleArn": "string",
  "auditNotificationTargetConfigurations": {
    "string": {
      "targetArn": "string",
      "roleArn": "string",
      "enabled": "boolean"
    }
  }
}
```
```json
{
  "auditCheckConfigurations": {
    "string": {
      "enabled": "boolean"
    }
  }
}
```

### Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>RoleArn</td>
<td>no</td>
<td>The ARN of the role that grants permission to AWS IoT to access information about your devices, policies, certificates and other items as necessary when performing an audit.</td>
</tr>
<tr>
<td>auditNotificationTargetConfigurations</td>
<td>AuditNotificationTargetConfigurations</td>
<td>no</td>
<td>Information about the targets to which audit notifications are sent.</td>
</tr>
<tr>
<td>auditCheckConfigurations</td>
<td>AuditCheckConfigurations</td>
<td>no</td>
<td>Specifies which audit checks are enabled and disabled for this account. Use DescribeAccountAuditConfiguration to see the list of all checks including those that are currently enabled. Note that some data collection may begin immediately when certain checks are enabled. When a check is disabled, any data collected so far in relation to the check is deleted. You cannot disable a check if it is used by any scheduled audit. You must first delete the check from the scheduled audit or delete the scheduled audit itself. On the first call to UpdateAccountAuditConfiguration this parameter is required and must</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Req?</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------</td>
<td>------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>specify at least one enabled check.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

**cli**

**Synopsis:**

```bash
aws iot update-account-audit-configuration \
    [--role-arn <value>] \
    [--audit-notification-target-configurations <value>] \
    [--audit-check-configurations <value>] \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
  "roleArn": "string",
  "auditNotificationTargetConfigurations": {
    "string": {
      "targetArn": "string",
      "roleArn": "string",
      "enabled": "boolean"
    }
  },
  "auditCheckConfigurations": {
    "string": {
      "enabled": "boolean"
    }
  }
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants permission to AWS IoT to</td>
</tr>
</tbody>
</table>
## Manage Audit Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>length- max:2048 min:20</td>
<td></td>
<td>access information about your devices, policies, certificates and other items as necessary when performing an audit.</td>
</tr>
<tr>
<td>auditNotificationTargetConfiguration</td>
<td>map</td>
<td>Information about the targets to which audit notifications are sent.</td>
</tr>
<tr>
<td>targetArn</td>
<td>string</td>
<td>The ARN of the target (SNS topic) to which audit notifications are sent.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants permission to send notifications to the target.</td>
</tr>
<tr>
<td>enabled</td>
<td>boolean</td>
<td>True if notifications to the target are enabled.</td>
</tr>
<tr>
<td>auditCheckConfigurations</td>
<td>map</td>
<td>Specifies which audit checks are enabled and disabled for this account. Use DescribeAccountAuditConfiguration to see the list of all checks including those that are currently enabled.</td>
</tr>
<tr>
<td>enabled</td>
<td>boolean</td>
<td>True if this audit check is enabled for this account.</td>
</tr>
</tbody>
</table>

Output:
None

Errors:
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

DescribeAccountAuditConfiguration

https

Request syntax:

GET /audit/configuration

Response syntax:

Content-type: application/json

```
{
  "roleArn": "string",
  "auditNotificationTargetConfigurations": {
    "string": {
      "targetArn": "string",
      "roleArn": "string",
      "enabled": "boolean"
    }
  },
  "auditCheckConfigurations": {
    "string": {
      "enabled": "boolean"
    }
  }
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>RoleArn</td>
<td>no</td>
<td>The ARN of the role that grants permission to AWS IoT to access information about your devices, policies, certificates and other items as necessary when performing an audit.</td>
</tr>
</tbody>
</table>

On the first call to UpdateAccountAuditConfiguration
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>this parameter is required.</td>
</tr>
<tr>
<td>auditNotificationTargetConfigurations</td>
<td>AuditNotificationTargetConfigurations</td>
<td>no</td>
<td>Information about the targets to which audit notifications are sent for this account.</td>
</tr>
<tr>
<td>auditCheckConfigurations</td>
<td>AuditCheckConfigurations</td>
<td>no</td>
<td>Which audit checks are enabled and disabled for this account.</td>
</tr>
</tbody>
</table>

**Errors:**

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

**cli**

**Synopsis:**

```bash
aws iot describe-account-audit-configuration \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
}
```

**Output:**

```json
{
    "roleArn": "string",
    "auditNotificationTargetConfigurations": {
        "string": {
            "targetArn": "string",
            "roleArn": "string",
            "enabled": "boolean"
        }
    },
    "auditCheckConfigurations": {
        "string": {
            "enabled": "boolean"
        }
    }
}
```
cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants permission to AWS IoT to access information about your devices, policies, certificates and other items as necessary when performing an audit. On the first call to <code>UpdateAccountAuditConfiguration</code> this parameter is required.</td>
</tr>
<tr>
<td>auditNotificationTargetConfigurationsmap</td>
<td>Information about the targets to which audit notifications are sent for this account.</td>
<td></td>
</tr>
<tr>
<td>targetArn</td>
<td>string</td>
<td>The ARN of the target (SNS topic) to which audit notifications are sent.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants permission to send notifications to the target.</td>
</tr>
<tr>
<td>enabled</td>
<td>boolean</td>
<td>True if notifications to the target are enabled.</td>
</tr>
<tr>
<td>auditCheckConfigurations</td>
<td>map</td>
<td>Which audit checks are enabled and disabled for this account.</td>
</tr>
<tr>
<td>enabled</td>
<td>boolean</td>
<td>True if this audit check is enabled for this account.</td>
</tr>
</tbody>
</table>

Errors:

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

**DeleteAccountAuditConfiguration**

Restores the default settings for Device Defender audits for this account. Any configuration data you entered is deleted and all audit checks are reset to disabled.

https

Request syntax:

```
DELETE /audit/configuration?deleteScheduledAudits=deleteScheduledAudits
```
URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deleteScheduledAudits</td>
<td>DeleteScheduledAudits</td>
<td>no</td>
<td>If true, all scheduled audits are deleted.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException
The specified resource does not exist.

HTTP response code: 404

ThrottlingException
The rate exceeds the limit.

HTTP response code: 429

InternalFailureException
An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot delete-account-audit-configuration
   [--delete-scheduled-audits --no-delete-scheduled-audits]
   [--cli-input-json <value>]
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "deleteScheduledAudits": "boolean"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deleteScheduledAudits</td>
<td>boolean</td>
<td>If true, all scheduled audits are deleted.</td>
</tr>
</tbody>
</table>

Output:
Schedule Audits

Create one or more scheduled audits using CreateScheduledAudit. This command allows you to specify the checks you want to perform during an audit and how often the audit should be run.

Keep track of your scheduled audits with ListScheduledAudits and DescribeScheduledAudit.

Change an existing scheduled audit with UpdateScheduledAudit or delete it with DeleteScheduledAudit.

CreateScheduledAudit

Creates a scheduled audit that is run at a specified time interval.

**Request syntax:**

```plaintext
POST /audit/scheduledaudits/
scheduledAuditName

Content-type: application/json

{
  "frequency": "string",
  "dayOfMonth": "string",
  "dayOfWeek": "string",
  "targetCheckNames": [
    "string"
  ]
}
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditName</td>
<td>ScheduledAuditName</td>
<td>yes</td>
<td>The name you want to give to the scheduled audit. (Max. 128 chars)</td>
</tr>
</tbody>
</table>
## Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>AuditFrequency</td>
<td>yes</td>
<td>How often the scheduled audit takes place. Can be one of &quot;DAILY&quot;, &quot;WEEKLY&quot;, &quot;BIWEEKLY&quot; or &quot;MONTHLY&quot;. The actual start time of each audit is determined by the system.</td>
</tr>
<tr>
<td>dayOfMonth</td>
<td>DayOfMonth</td>
<td>no</td>
<td>The day of the month on which the scheduled audit takes place. Can be &quot;1&quot; through &quot;31&quot; or &quot;LAST&quot;. This field is required if the &quot;frequency&quot; parameter is set to &quot;MONTHLY&quot;. If days 29-31 are specified, and the month does not have that many days, the audit takes place on the &quot;LAST&quot; day of the month.</td>
</tr>
<tr>
<td>dayOfWeek</td>
<td>DayOfWeek</td>
<td>no</td>
<td>The day of the week on which the scheduled audit takes place. Can be one of &quot;SUN&quot;, &quot;MON&quot;, &quot;TUE&quot;, &quot;WED&quot;, &quot;THU&quot;, &quot;FRI&quot; or &quot;SAT&quot;. This field is required if the &quot;frequency&quot; parameter is set to &quot;WEEKLY&quot; or &quot;BIWEEKLY&quot;.</td>
</tr>
<tr>
<td>targetCheckNames</td>
<td>TargetAuditCheckNames</td>
<td>yes</td>
<td>Which checks are performed during the scheduled audit. Checks must be enabled for your account. (Use DescribeAccountAuditConfiguration to see the list of all checks including those that are enabled or UpdateAccountAuditConfiguration to select which checks are enabled.)</td>
</tr>
</tbody>
</table>

**Response syntax:**
Content-type: application/json

```json
{
  "scheduledAuditArn": "string"
}
```

### Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditArn</td>
<td>ScheduledAuditArn</td>
<td>no</td>
<td>The ARN of the scheduled audit.</td>
</tr>
</tbody>
</table>

### Errors:

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

**LimitExceededException**

A limit has been exceeded.

HTTP response code: 410

---

### Synopsis:

```
aws iot create-scheduled-audit \
  --frequency <value> \
  [--day-of-month <value>] \ 
  [--day-of-week <value>] \
  --target-check-names <value> \ 
  --scheduled-audit-name <value> \ 
  [--cli-input-json <value>] \ 
  [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
  "frequency": "string",
}
cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>string</td>
<td>How often the scheduled audit takes place. Can be one of &quot;DAILY&quot;, &quot;WEEKLY&quot;, &quot;BIWEEKLY&quot; or &quot;MONTHLY&quot;. The actual start time of each audit is determined by the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: DAILY</td>
</tr>
<tr>
<td>dayOfMonth</td>
<td>string</td>
<td>The day of the month on which the scheduled audit takes place. Can be &quot;1&quot; through &quot;31&quot; or &quot;LAST&quot;. This field is required if the &quot;frequency&quot; parameter is set to &quot;MONTHLY&quot;. If days 29-31 are specified, and the month does not have that many days, the audit takes place on the &quot;LAST&quot; day of the month.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pattern: ^([1-9]</td>
</tr>
<tr>
<td>dayOfWeek</td>
<td>string</td>
<td>The day of the week on which the scheduled audit takes place. Can be one of &quot;SUN&quot;, &quot;MON&quot;, &quot;TUE&quot;, &quot;WED&quot;, &quot;THU&quot;, &quot;FRI&quot; or &quot;SAT&quot;. This field is required if the &quot;frequency&quot; parameter is set to &quot;WEEKLY&quot; or &quot;BIWEEKLY&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: SUN</td>
</tr>
<tr>
<td>targetCheckNames</td>
<td>list</td>
<td>Which checks are performed during the scheduled audit. Checks must be enabled for your account. (Use DescribeAccountAuditConfiguration to see the list of all checks including those that are enabled or UpdateAccountAuditConfiguration to select which checks are enabled.)</td>
</tr>
<tr>
<td>member: AuditCheckName</td>
<td></td>
<td></td>
</tr>
<tr>
<td>scheduledAuditName</td>
<td>string</td>
<td>The name you want to give to the scheduled audit. (Max. 128 chars)</td>
</tr>
</tbody>
</table>
### Schedule Audits

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pattern: [a-zA-Z0-9_-]+</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
  "scheduledAuditArn": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditArn</td>
<td>string</td>
<td>The ARN of the scheduled audit.</td>
</tr>
</tbody>
</table>

**Errors:**

- **InvalidRequestException**
  
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ThrottlingException**
  
The rate exceeds the limit.

- **InternalFailureException**
  
  An unexpected error has occurred.

- **LimitExceededException**
  
  A limit has been exceeded.

### ListScheduledAudits

Lists all of your scheduled audits.

https

**Request syntax:**

```
GET /audit/scheduledaudits?maxResults=maxResults&nextToken=nextToken
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time. The default is 25.</td>
</tr>
</tbody>
</table>
Response syntax:

Content-type: application/json

```json
{
    "scheduledAudits": [
        {
            "scheduledAuditName": "string",
            "scheduledAuditArn": "string",
            "frequency": "string",
            "dayOfMonth": "string",
            "dayOfWeek": "string"
        }
    ],
    "nextToken": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAudits</td>
<td>ScheduledAuditMetadataList</td>
<td>no</td>
<td>The list of scheduled audits.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```bash
aws iot list-scheduled-audits
```
Schedule Audits

[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]

**cli-input-json format:**

```json
{
  "nextToken": "string",
  "maxResults": "integer"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time. The default is 25.</td>
</tr>
<tr>
<td></td>
<td>range- max:250 min:1</td>
<td></td>
</tr>
</tbody>
</table>

**Output:**

```json
{
  "scheduledAudits": [
  {
    "scheduledAuditName": "string",
    "scheduledAuditArn": "string",
    "frequency": "string",
    "dayOfMonth": "string",
    "dayOfWeek": "string"
  }
  ],
  "nextToken": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAudits</td>
<td>list</td>
<td>The list of scheduled audits.</td>
</tr>
<tr>
<td>member</td>
<td>ScheduledAuditMetadata</td>
<td></td>
</tr>
<tr>
<td>java class: java.util.List</td>
<td></td>
<td></td>
</tr>
<tr>
<td>scheduledAuditName</td>
<td>string</td>
<td>The name of the scheduled audit.</td>
</tr>
<tr>
<td>length- max:128 min:1</td>
<td>pattern: [a-zA-Z0-9_-]+</td>
<td></td>
</tr>
<tr>
<td>scheduledAuditArn</td>
<td>string</td>
<td>The ARN of the scheduled audit.</td>
</tr>
<tr>
<td>frequency</td>
<td>string</td>
<td>How often the scheduled audit takes place.</td>
</tr>
</tbody>
</table>
Schedule Audits

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
</tbody>
</table>
| Type          | enum: DAILY | WEEKLY | BIWEEKLY | MONTHLY
| Description   | string          | The day of the month on which the scheduled audit is run (if the frequency is "MONTHLY"). If days 29-31 are specified, and the month does not have that many days, the audit takes place on the "LAST" day of the month. |
| dayOfMonth    | string          | The day of the week on which the scheduled audit is run (if the frequency is "WEEKLY" or "BIWEEKLY"). |
| dayOfWeek     | string          | The day of the week on which the scheduled audit is run (if the frequency is "WEEKLY" or "BIWEEKLY"). |
| nextToken     | string          | A token that can be used to retrieve the next set of results, or null if there are no additional results. |

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

DescribeScheduledAudit

Gets information about a scheduled audit.

https

Request syntax:

```
GET /audit/scheduledaudits/scheduledAuditName
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditName</td>
<td>ScheduledAuditName</td>
<td>yes</td>
<td>The name of the scheduled audit whose</td>
</tr>
</tbody>
</table>

426
Schedule Audits

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>AuditFrequency</td>
<td>no</td>
<td>How often the scheduled audit takes place. One of &quot;DAILY&quot;, &quot;WEEKLY&quot;, &quot;BIWEEKLY&quot; or &quot;MONTHLY&quot;. The actual start time of each audit is determined by the system.</td>
</tr>
<tr>
<td>dayOfMonth</td>
<td>DayOfMonth</td>
<td>no</td>
<td>The day of the month on which the scheduled audit takes place. Will be &quot;1&quot; through &quot;31&quot; or &quot;LAST&quot;. If days 29-31 are specified, and the month does not have that many days, the audit takes place on the &quot;LAST&quot; day of the month.</td>
</tr>
<tr>
<td>dayOfWeek</td>
<td>DayOfWeek</td>
<td>no</td>
<td>The day of the week on which the scheduled audit takes place. One of &quot;SUN&quot;, &quot;MON&quot;, &quot;TUE&quot;, &quot;WED&quot;, &quot;THU&quot;, &quot;FRI&quot; or &quot;SAT&quot;.</td>
</tr>
<tr>
<td>targetCheckNames</td>
<td>TargetAuditCheckNames</td>
<td>no</td>
<td>Which checks are performed during the scheduled audit. (Note that checks</td>
</tr>
</tbody>
</table>

Response syntax:

```json
Content-type: application/json
{
"frequency": "string",
"dayOfMonth": "string",
"dayOfWeek": "string",
"targetCheckNames": [
  "string"
],
"scheduledAuditName": "string",
"scheduledAuditArn": "string"
}
```

Response Body Parameters:
Schedule Audits

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditName</td>
<td>ScheduledAuditName</td>
<td>no</td>
<td>The name of the scheduled audit.</td>
</tr>
<tr>
<td>scheduledAuditArn</td>
<td>ScheduledAuditArn</td>
<td>no</td>
<td>The ARN of the scheduled audit.</td>
</tr>
</tbody>
</table>

**Errors:**

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

ci

**Synopsis:**

```
aws iot describe-scheduled-audit \
  --scheduled-audit-name <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "scheduledAuditName": "string"
}
```
cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditName</td>
<td>string</td>
<td>The name of the scheduled audit whose information you want to get.</td>
</tr>
<tr>
<td></td>
<td>length-</td>
<td>max:128 min:1</td>
</tr>
<tr>
<td></td>
<td>pattern:</td>
<td>[a-zA-Z0-9-_]+</td>
</tr>
</tbody>
</table>

Output:

```json
{
  "frequency": "string",
  "dayOfMonth": "string",
  "dayOfWeek": "string",
  "targetCheckNames": [
    "string"
  ],
  "scheduledAuditName": "string",
  "scheduledAuditArn": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>string</td>
<td>How often the scheduled audit takes place. One of &quot;DAILY&quot;, &quot;WEEKLY&quot;, &quot;BIWEEKLY&quot; or &quot;MONTHLY&quot;. The actual start time of each audit is determined by the system.</td>
</tr>
<tr>
<td></td>
<td>enum:</td>
<td>DAILY</td>
</tr>
<tr>
<td>dayOfMonth</td>
<td>string</td>
<td>The day of the month on which the scheduled audit takes place. Will be &quot;1&quot; through &quot;31&quot; or &quot;LAST&quot;. If days 29-31 are specified, and the month does not have that many days, the audit takes place on the &quot;LAST&quot; day of the month.</td>
</tr>
<tr>
<td></td>
<td>pattern:</td>
<td>^([1-9]</td>
</tr>
<tr>
<td>dayOfWeek</td>
<td>string</td>
<td>The day of the week on which the scheduled audit takes place. One of &quot;SUN&quot;, &quot;MON&quot;, &quot;TUE&quot;, &quot;WED&quot;, &quot;THU&quot;, &quot;FRI&quot; or &quot;SAT&quot;.</td>
</tr>
<tr>
<td></td>
<td>enum:</td>
<td>SUN</td>
</tr>
<tr>
<td>targetCheckNames</td>
<td>list</td>
<td>Which checks are performed during the scheduled audit.</td>
</tr>
</tbody>
</table>
Schedule Audits

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditName</td>
<td>string</td>
<td>The name of the scheduled audit.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>scheduledAuditArn</td>
<td>string</td>
<td>The ARN of the scheduled audit.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceNotFoundException

The specified resource does not exist.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

UpdateScheduledAudit

Updates a scheduled audit, including what checks are performed and how often the audit takes place.

https

Request syntax:

```
PATCH /audit/scheduledaudits/scheduledAuditName
Content-type: application/json

{
  "frequency": "string",
  "dayOfMonth": "string",
  "dayOfWeek": "string",
  "targetCheckNames": [ "string"
}
```
### URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditName</td>
<td>ScheduledAuditName</td>
<td>yes</td>
<td>The name of the scheduled audit. (Max. 128 chars)</td>
</tr>
</tbody>
</table>

### Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>AuditFrequency</td>
<td>no</td>
<td>How often the scheduled audit takes place. Can be one of &quot;DAILY&quot;, &quot;WEEKLY&quot;, &quot;BIWEEKLY&quot; or &quot;MONTHLY&quot;. The actual start time of each audit is determined by the system.</td>
</tr>
<tr>
<td>dayOfMonth</td>
<td>DayOfMonth</td>
<td>no</td>
<td>The day of the month on which the scheduled audit takes place. Can be &quot;1&quot; through &quot;31&quot; or &quot;LAST&quot;. This field is required if the frequency parameter is set to &quot;MONTHLY&quot;. If days 29-31 are specified, and the month does not have that many days, the audit takes place on the &quot;LAST&quot; day of the month.</td>
</tr>
<tr>
<td>dayOfWeek</td>
<td>DayOfWeek</td>
<td>no</td>
<td>The day of the week on which the scheduled audit takes place. Can be one of &quot;SUN&quot;, &quot;MON&quot;, &quot;TUE&quot;, &quot;WED&quot;, &quot;THU&quot;, &quot;FRI&quot; or &quot;SAT&quot;. This field is required if the frequency parameter is set to &quot;WEEKLY&quot; or &quot;BIWEEKLY&quot;.</td>
</tr>
<tr>
<td>targetCheckNames</td>
<td>TargetAuditCheckNames</td>
<td>no</td>
<td>Which checks are performed during the scheduled audit. Checks must be enabled for your account. (Use DescribeAccountAuditConfiguration to see the list of all</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Req?</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------</td>
<td>------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>checks including those that are enabled or UpdateAccountAuditConfiguration to select which checks are enabled.</td>
</tr>
</tbody>
</table>

Response syntax:

```json
{  "scheduledAuditArn": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditArn</td>
<td>ScheduledAuditArn</td>
<td>no</td>
<td>The ARN of the scheduled audit.</td>
</tr>
</tbody>
</table>

Errors:

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

cli

**Synopsis:**

```
aws iot update-scheduled-audit \  
    [--frequency <value>] \  
    [--day-of-month <value>] \
```
Schedule Audits

[--day-of-week <value>] \
[--target-check-names <value>] \
[--scheduled-audit-name <value>] \ 
[--cli-input-json <value>] \ 
[--generate-cli-skeleton]

**cli-input-json format:**

```
{
    "frequency": "string",
    "dayOfMonth": "string",
    "dayOfWeek": "string",
    "targetCheckNames": [
        "string"
    ],
    "scheduledAuditName": "string"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>string</td>
<td>How often the scheduled audit takes place. Can be one of &quot;DAILY&quot;, &quot;WEEKLY&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;BIWEEKLY&quot; or &quot;MONTHLY&quot;. The actual start time of each audit is determined</td>
</tr>
<tr>
<td></td>
<td></td>
<td>by the system. enum: DAILY</td>
</tr>
<tr>
<td>dayOfMonth</td>
<td>string</td>
<td>The day of the month on which the scheduled audit takes place. Can be &quot;1&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>through &quot;31&quot; or &quot;LAST&quot;. This field is required if the &quot;frequency&quot; parameter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>is set to &quot;MONTHLY&quot;. If days 29–31 are specified, and the month does not</td>
</tr>
<tr>
<td></td>
<td></td>
<td>have that many days, the audit takes place on the &quot;LAST&quot; day of the month.</td>
</tr>
<tr>
<td>dayOfWeek</td>
<td>string</td>
<td>The day of the week on which the scheduled audit takes place. Can be one of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;SUN&quot;, &quot;MON&quot;, &quot;TUE&quot;, &quot;WED&quot;, &quot;THU&quot;, &quot;FRI&quot; or &quot;SAT&quot;. This field is required if</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the &quot;frequency&quot; parameter is set to &quot;WEEKLY&quot; or &quot;BIWEEKLY&quot;. enum: SUN</td>
</tr>
<tr>
<td>targetCheckNames</td>
<td>list</td>
<td>Which checks are performed during the scheduled audit. Checks must be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enabled for your account. (Use DescribeAccountAuditConfiguration.)</td>
</tr>
</tbody>
</table>
Schedule Audits

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditName</td>
<td>string</td>
<td>The name of the scheduled audit. (Max. 128 chars)</td>
</tr>
<tr>
<td></td>
<td>length: max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
  "scheduledAuditArn": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditArn</td>
<td>string</td>
<td>The ARN of the scheduled audit.</td>
</tr>
</tbody>
</table>

Errors:

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ResourceNotFoundException**
  
  The specified resource does not exist.

- **ThrottlingException**
  
  The rate exceeds the limit.

- **InternalFailureException**
  
  An unexpected error has occurred.

**DeleteScheduledAudit**

Deletes a scheduled audit.

```plaintext
https
```

Request syntax:

```
DELETE /audit/scheduledaudits/scheduledAuditName
```
URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditName</td>
<td>ScheduledAuditName</td>
<td>yes</td>
<td>The name of the scheduled audit you want to delete.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

aws iot delete-scheduled-audit \
   --scheduled-audit-name <value> \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]

cli-input-json format:

```
{
   "scheduledAuditName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditName</td>
<td>string</td>
<td>The name of the scheduled audit you want to delete.</td>
</tr>
</tbody>
</table>

length- max:128 min:1

pattern: [a-zA-Z0-9_]+
Run An On-Demand Audit

Use `StartOnDemandAuditTask` to specify the checks you want to perform and start an audit running right away.

**StartOnDemandAuditTask**

Starts an on-demand Device Defender audit.

**Request syntax:**

```
POST /audit/tasks
Content-type: application/json

{
   "targetCheckNames": [
      "string"
   ]
}
```

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targetCheckNames</td>
<td>TargetAuditCheckNames</td>
<td>yes</td>
<td>Which checks are performed during the audit. The checks you specify must be enabled for your account or an exception occurs. Use <code>DescribeAccountAuditConfiguration</code> to see the list of all checks including those</td>
</tr>
</tbody>
</table>
Run An On-Demand Audit

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>that are enabled or UpdateAccountAuditConfiguration to select which checks are enabled.</td>
</tr>
</tbody>
</table>

Response syntax:

```
Content-type: application/json
{
  "taskId": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>AuditTaskId</td>
<td>no</td>
<td>The ID of the on-demand audit you started.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException
The rate exceeds the limit.

HTTP response code: 429

InternalFailureException
An unexpected error has occurred.

HTTP response code: 500

LimitExceededException
A limit has been exceeded.

HTTP response code: 410

cli

Synopsis:

```
aws iot start-on-demand-audit-task
```
Run An On-Demand Audit

```
--target-check-names <value>  
[--cli-input-json <value>]  
[--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "targetCheckNames": [
    "string"
  ]
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targetCheckNames</td>
<td>list</td>
<td>Which checks are performed during the audit. The checks you specify must be enabled for your account or an exception occurs. Use DescribeAccountAuditConfiguration to see the list of all checks including those that are enabled or UpdateAccountAuditConfiguration to select which checks are enabled.</td>
</tr>
</tbody>
</table>

Output:

```
{
  "taskId": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>string</td>
<td>The ID of the on-demand audit you started.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.
InternalFailureException
An unexpected error has occurred.
LimitExceeded Exception
A limit has been exceeded.

Manage Audit Instances

Use DescribeAuditTask to get information about a specific audit instance. If it has already run, the results include which checks failed and which passed, those that the system was unable to complete, and if the audit is still in progress, those it is still working on.

Use ListAuditTasks to find the audits that were run during a specific time interval.

Use CancelAuditTask to halt an audit in progress.

DescribeAuditTask

Gets information about a Device Defender audit.

https

Request syntax:

GET /audit/tasks/taskId

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>AuditTaskId</td>
<td>yes</td>
<td>The ID of the audit whose information you want to get.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{  
  "taskStatus": "string",
  "taskType": "string",
  "taskStartTime": "timestamp",
  "taskStatistics": {
    "totalChecks": "integer",
    "inProgressChecks": "integer",
    "waitingForDataCollectionChecks": "integer",
    "compliantChecks": "integer",
    "nonCompliantChecks": "integer",
    "failedChecks": "integer",
    "canceledChecks": "integer"
  },
  "scheduledAuditName": "string",
  "auditDetails": {
    "string": {
      "string": {

439
"checkRunStatus": "string",
"checkCompliant": "boolean",
"totalResourcesCount": "long",
"nonCompliantResourcesCount": "long",
"errorCode": "string",
"message": "string"
}
}
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskStatus</td>
<td>AuditTaskStatus</td>
<td>no</td>
<td>The status of the audit: one of &quot;IN_PROGRESS&quot;, &quot;COMPLETED&quot;, &quot;FAILED&quot;, or &quot;CANCELED&quot;.</td>
</tr>
<tr>
<td>taskType</td>
<td>AuditTaskType</td>
<td>no</td>
<td>The type of audit: &quot;ON_DEMAND_AUDIT_TASK&quot; or &quot;SCHEDULED_AUDIT_TASK&quot;.</td>
</tr>
<tr>
<td>taskStartTime</td>
<td>Timestamp</td>
<td>no</td>
<td>The time the audit started.</td>
</tr>
<tr>
<td>taskStatistics</td>
<td>TaskStatistics</td>
<td>no</td>
<td>Statistical information about the audit.</td>
</tr>
<tr>
<td>scheduledAuditName</td>
<td>ScheduledAuditName</td>
<td>no</td>
<td>The name of the scheduled audit (only if the audit was a scheduled audit).</td>
</tr>
<tr>
<td>auditDetails</td>
<td>AuditDetails</td>
<td>no</td>
<td>Detailed information about each check performed during this audit.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

440
HTTP response code: 429
InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

cli

Synopsis:

```
aws iot describe-audit-task \
--task-id <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "taskId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>string</td>
<td>The ID of the audit whose information you want to get.</td>
</tr>
<tr>
<td></td>
<td>length- max:40 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```
{
  "taskStatus": "string",
  "taskType": "string",
  "taskStartTime": "timestamp",
  "taskStatistics": {
    "totalChecks": "integer",
    "inProgressChecks": "integer",
    "waitingForDataCollectionChecks": "integer",
    "compliantChecks": "integer",
    "nonCompliantChecks": "integer",
    "failedChecks": "integer",
    "canceledChecks": "integer"
  },
  "scheduledAuditName": "string",
  "auditDetails": {
    "string": {
      "checkRunStatus": "string",
      "checkCompliant": "boolean",
      "totalResourcesCount": "long",
      "nonCompliantResourcesCount": "long",
      "errorCode": "string",
      "message": "string"
    }
  }
}
```
cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskStatus</td>
<td>string</td>
<td>The status of the audit: one of &quot;IN_PROGRESS&quot;, &quot;COMPLETED&quot;, &quot;FAILED&quot;, or &quot;CANCELED&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>taskType</td>
<td>string</td>
<td>The type of audit: &quot;ON_DEMAND_AUDIT_TASK&quot; or &quot;SCHEDULED_AUDIT_TASK&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>taskStartTime</td>
<td>timestamp</td>
<td>The time the audit started.</td>
</tr>
<tr>
<td>taskStatistics</td>
<td>TaskStatistics</td>
<td>Statistical information about the audit.</td>
</tr>
<tr>
<td>totalChecks</td>
<td>integer</td>
<td>The number of checks in this audit.</td>
</tr>
<tr>
<td>inProgressChecks</td>
<td>integer</td>
<td>The number of checks in progress.</td>
</tr>
<tr>
<td>waitingForDataCollectionChecks</td>
<td>integer</td>
<td>The number of checks waiting for data collection.</td>
</tr>
<tr>
<td>compliantChecks</td>
<td>integer</td>
<td>The number of checks that found compliant resources.</td>
</tr>
<tr>
<td>nonCompliantChecks</td>
<td>integer</td>
<td>The number of checks that found non-compliant resources.</td>
</tr>
<tr>
<td>failedChecks</td>
<td>integer</td>
<td>The number of checks</td>
</tr>
<tr>
<td>canceledChecks</td>
<td>integer</td>
<td>The number of checks that did not run because the audit was canceled.</td>
</tr>
<tr>
<td>scheduledAuditName</td>
<td>string</td>
<td>The name of the scheduled audit (only if the audit was a scheduled audit).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>auditDetails</td>
<td>map</td>
<td>Detailed information about each check performed during this audit.</td>
</tr>
<tr>
<td>checkRunStatus</td>
<td>string</td>
<td>The completion status of this check, one of &quot;IN_PROGRESS&quot;, &quot;COMPLETED&quot;, &quot;FAILED&quot;, or &quot;CANCELED&quot;.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td>&quot;WAITING_FOR_DATA_COLLECTION&quot;, &quot;CANCELED&quot;, &quot;COMPLETED_COMPLIANT&quot;, &quot;COMPLETED_NON_COMPLIANT&quot;, or &quot;FAILED&quot;. enum: IN_PROGRESS</td>
</tr>
<tr>
<td>checkCompliant</td>
<td>boolean</td>
<td>True if the check completed and found all resources compliant.</td>
</tr>
<tr>
<td>totalResourcesCount</td>
<td>long</td>
<td>The number of resources on which the check was performed.</td>
</tr>
<tr>
<td>nonCompliantResourcesCount</td>
<td>long</td>
<td>The number of resources that the check found non-compliant.</td>
</tr>
<tr>
<td>errorCode</td>
<td>string</td>
<td>The code of any error encountered when performing this check during this audit. One of &quot;INSUFFICIENT_PERMISSIONS&quot;, or &quot;AUDIT_CHECK_DISABLED&quot;.</td>
</tr>
<tr>
<td>message</td>
<td>string</td>
<td>length- max:2048 The message associated with any error encountered when performing this check during this audit.</td>
</tr>
</tbody>
</table>

**Errors:**

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceNotFoundException

The specified resource does not exist.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

**ListAuditTasks**

Lists the Device Defender audits that have been performed during a given time period.
Request syntax:

GET /audit/tasks?
maxResults=maxResults&nextToken=nextToken&taskStatus=taskStatus&taskType=taskType&startTime=startTime&endTime=endTime

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startTime</td>
<td>Timestamp</td>
<td>yes</td>
<td>The beginning of the time period. Note that audit information is retained for a limited time (180 days). Requesting a start time prior to what is retained results in an &quot;InvalidRequestException&quot;.</td>
</tr>
<tr>
<td>endTime</td>
<td>Timestamp</td>
<td>yes</td>
<td>The end of the time period.</td>
</tr>
<tr>
<td>taskType</td>
<td>AuditTaskType</td>
<td>no</td>
<td>A filter to limit the output to the specified type of audit: can be one of &quot;ON_DEMAND_AUDIT_TASK&quot; or &quot;SCHEDULED_AUDIT_TASK&quot;.</td>
</tr>
<tr>
<td>taskStatus</td>
<td>AuditTaskStatus</td>
<td>no</td>
<td>A filter to limit the output to audits with the specified completion status: can be one of &quot;IN_PROGRESS&quot;, &quot;COMPLETED&quot;, &quot;FAILED&quot; or &quot;CANCELED&quot;.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time. The default is 25.</td>
</tr>
</tbody>
</table>

Response syntax:

```
Content-type: application/json

{
  "tasks": [
    {
      "taskId": "string",
    }
  ]
```

"taskStatus": "string",
  "taskType": "string"
}]
  "nextToken": "string"
}

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tasks</td>
<td>AuditTaskMetadataList</td>
<td>no</td>
<td>The audits that were performed during the specified time period.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

**Errors:**

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

**cli**

**Synopsis:**

```
aws iot list-audit-tasks \
  --start-time <value> \
  --end-time <value> \
  [--task-type <value>] \
  [--task-status <value>] \
  [--next-token <value>] \
  [--max-results <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
```
"startTime": "timestamp",
"endTime": "timestamp",
"taskType": "string",
"taskStatus": "string",
"nextToken": "string",
"maxResults": "integer"
}

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startTime</td>
<td>timestamp</td>
<td>The beginning of the time period. Note that audit information is retained for a limited time (180 days). Requesting a start time prior to what is retained results in an &quot;InvalidRequestException&quot;.</td>
</tr>
<tr>
<td>endTime</td>
<td>timestamp</td>
<td>The end of the time period.</td>
</tr>
<tr>
<td>taskType</td>
<td>string</td>
<td>A filter to limit the output to the specified type of audit: can be one of &quot;ON_DEMAND_AUDIT_TASK&quot; or &quot;SCHEDULED_AUDIT_TASK&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: ON_DEMAND_AUDIT_TASK</td>
</tr>
<tr>
<td>taskStatus</td>
<td>string</td>
<td>A filter to limit the output to audits with the specified completion status: can be one of &quot;IN_PROGRESS&quot;, &quot;COMPLETED&quot;, &quot;FAILED&quot; or &quot;CANCELED&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: IN_PROGRESS</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time. The default is 25.</td>
</tr>
<tr>
<td></td>
<td>range: max:250 min:1</td>
<td></td>
</tr>
</tbody>
</table>

**Output:**

```json
{
  "tasks": [
    {
      "taskId": "string",
      "taskStatus": "string",
      "taskType": "string"
    }
  ],
```
"nextToken": "string"
}

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tasks</td>
<td>list</td>
<td>The audits that were performed during the specified time period.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>member: AuditTaskMetadata</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java class: java.util.List</td>
</tr>
<tr>
<td>taskld</td>
<td>string</td>
<td>The ID of this audit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>length- max:40 min:1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pattern: [a-zA-Z0-9-]+</td>
</tr>
<tr>
<td>taskStatus</td>
<td>string</td>
<td>The status of this audit: one of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;IN_PROGRESS&quot;, &quot;COMPLETED&quot;, &quot;FAILED&quot; or &quot;CANCELED&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: IN_PROGRESS</td>
</tr>
<tr>
<td>taskType</td>
<td>string</td>
<td>The type of this audit: one of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;ON_DEMAND_AUDIT_TASK&quot; or &quot;SCHEDULED_AUDIT_TASK&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: ON_DEMAND_AUDIT_TASK</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

CancelAuditTask

Cancels an audit that is in progress. The audit can be either scheduled or on-demand. If the audit is not in progress, an "InvalidRequestException" occurs.
**Request syntax:**

```
PUT /audit/tasks/taskId/cancel
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>AuditTaskId</td>
<td>yes</td>
<td>The ID of the audit you want to cancel. You can only cancel an audit that is &quot;IN_PROGRESS&quot;.</td>
</tr>
</tbody>
</table>

**Errors:**

- **ResourceNotFoundException**
  
  The specified resource does not exist.

  HTTP response code: 404

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

  HTTP response code: 400

- **ThrottlingException**
  
  The rate exceeds the limit.

  HTTP response code: 429

- **InternalFailureException**
  
  An unexpected error has occurred.

  HTTP response code: 500

**cli**

**Synopsis:**

```
aws iot cancel-audit-task \
  --task-id <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
  "taskId": "string"
}
```
Check Audit Results

Use ListAuditFindings to see the results of an audit. You can filter the results by the type of check, a specific resource, or the time of the audit. Armed with this information, you can take the appropriate steps to mitigate any problems that were found.

ListAuditFindings

Lists the findings (results) of a Device Defender audit or of the audits performed during a specified time period. (Findings are retained for 180 days.)

https

Request syntax:

```
POST /audit/findings
Content-type: application/json

{
  "taskId": "string",
  "checkName": "string",
  "resourceIdentifier": {
    "deviceCertificateId": "string",
  }
}
```
"caCertificateId": "string",
"cognitoIdentityPoolId": "string",
"clientId": "string",
"policyVersionIdentifier": {
  "policyName": "string",
  "policyVersionId": "string"
},
"account": "string"
"maxResults": "integer",
"nextToken": "string",
"startTime": "timestamp",
"endTime": "timestamp"
}

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>AuditTaskId</td>
<td>no</td>
<td>A filter to limit results to the audit with the specified ID. You must specify either the taskId or the startTime and endTime, but not both.</td>
</tr>
<tr>
<td>checkName</td>
<td>AuditCheckName</td>
<td>no</td>
<td>A filter to limit results to the findings for the specified audit check.</td>
</tr>
<tr>
<td>resourceIdentifier</td>
<td>ResourceIdentifier</td>
<td>no</td>
<td>Information identifying the non-compliant resource.</td>
</tr>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time. The default is 25.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>startTime</td>
<td>Timestamp</td>
<td>no</td>
<td>A filter to limit results to those found after the specified time. You must specify either the startTime and endTime or the taskId, but not both.</td>
</tr>
<tr>
<td>endTime</td>
<td>Timestamp</td>
<td>no</td>
<td>A filter to limit results to those found before the specified time. You must specify either the startTime and endTime or the taskId, but not both.</td>
</tr>
</tbody>
</table>

Response syntax:
Content-type: application/json

{
    "findings": [
        {
            "taskId": "string",
            "checkName": "string",
            "taskStartTime": "timestamp",
            "findingTime": "timestamp",
            "severity": "string",
            "nonCompliantResource": {
                "resourceType": "string",
                "resourceIdentifier": {
                    "deviceCertificateId": "string",
                    "caCertificateId": "string",
                    "cognitoIdentityPoolId": "string",
                    "clientId": "string",
                    "policyVersionIdentifier": {
                        "policyName": "string",
                        "policyVersionId": "string"
                    },
                    "account": "string"
                },
                "additionalInfo": {
                    "string": "string"
                }
            },
            "relatedResources": [
                {
                    "resourceType": "string",
                    "resourceIdentifier": {
                        "deviceCertificateId": "string",
                        "caCertificateId": "string",
                        "cognitoIdentityPoolId": "string",
                        "clientId": "string",
                        "policyVersionIdentifier": {
                            "policyName": "string",
                            "policyVersionId": "string"
                        },
                        "account": "string"
                    },
                    "additionalInfo": {
                        "string": "string"
                    }
                }
            ],
            "reasonForNonCompliance": "string",
            "reasonForNonComplianceCode": "string"
        }
    ],
    "nextToken": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>findings</td>
<td>AuditFindings</td>
<td>no</td>
<td>The findings (results) of the audit.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token that can be used to retrieve the next set of results, or</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Req?</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------</td>
<td>------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>null</td>
<td>if there are no additional results.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Errors:

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```bash
aws iot list-audit-findings \
  [--task-id <value>] \ 
  [--check-name <value>] \ 
  [--resource-identifier <value>] \ 
  [--max-results <value>] \ 
  [--next-token <value>] \ 
  [--start-time <value>] \ 
  [--end-time <value>] \ 
  [--cli-input-json <value>] \ 
  [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "taskId": "string",
  "checkName": "string",
  "resourceIdentifier": {
    "deviceCertificateId": "string",
    "caCertificateId": "string",
    "cognitoIdentityPoolId": "string",
    "clientId": "string",
    "policyVersionIdentifier": {
      "policyName": "string",
      "policyVersionId": "string"
    },
    "account": "string"
  },
  "maxResults": "integer",
  "nextToken": "string",
  "startTime": "timestamp",
  "endTime": "timestamp"
}
```
### cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>string</td>
<td>A filter to limit results to the audit with the specified ID. You must specify either the taskId or the startTime and endTime, but not both.</td>
</tr>
<tr>
<td>checkName</td>
<td>string</td>
<td>A filter to limit results to the findings for the specified audit check.</td>
</tr>
<tr>
<td>resourceIdentifier</td>
<td>ResourceIdentifier</td>
<td>Information identifying the non-compliant resource.</td>
</tr>
<tr>
<td>deviceCertificateId</td>
<td>string</td>
<td>The ID of the certificate attached to the resource.</td>
</tr>
<tr>
<td>caCertificateId</td>
<td>string</td>
<td>The ID of the CA certificate used to authorize the certificate.</td>
</tr>
<tr>
<td>cognitoIdentityPoolId</td>
<td>string</td>
<td>The ID of the Cognito Identity Pool.</td>
</tr>
<tr>
<td>clientId</td>
<td>string</td>
<td>The client ID.</td>
</tr>
<tr>
<td>policyVersionIdentifier</td>
<td>PolicyVersionIdentifier</td>
<td>The version of the policy associated with the resource.</td>
</tr>
<tr>
<td>policyName</td>
<td>string</td>
<td>The name of the policy.</td>
</tr>
<tr>
<td>policyVersionId</td>
<td>string</td>
<td>The ID of the version of the policy associated with the resource.</td>
</tr>
<tr>
<td>account</td>
<td>string</td>
<td>The account with which the resource is associated.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time. The default is 25.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results.</td>
</tr>
</tbody>
</table>
Check Audit Results

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startTime</td>
<td>timestamp</td>
<td>A filter to limit results to those found after the specified time. You must specify either the startTime and endTime or the taskId, but not both.</td>
</tr>
<tr>
<td>endTime</td>
<td>timestamp</td>
<td>A filter to limit results to those found before the specified time. You must specify either the startTime and endTime or the taskId, but not both.</td>
</tr>
</tbody>
</table>

Output:

```json
{  
  "findings": [
    
    
    
    
    
    
    "taskId": "string",
    "checkName": "string",
    "taskStartTime": "timestamp",
    "findingTime": "timestamp",
    "severity": "string",
    "nonCompliantResource": {
      "resourceType": "string",
      "resourceIdentifier": {
        "deviceCertificateId": "string",
        "caCertificateId": "string",
        "cognitoIdentityPoolId": "string",
        "clientId": "string",
        "policyVersionIdentifier": {
          "policyName": "string",
          "policyVersionId": "string"
        },
        "account": "string"
      },
      "additionalInfo": {
        "string": "string"
      }
    },
    "relatedResources": [
      {
        "resourceType": "string",
        "resourceIdentifier": {
          "deviceCertificateId": "string",
          "caCertificateId": "string",
          "cognitoIdentityPoolId": "string",
          "clientId": "string",
          "policyVersionIdentifier": {
            "policyName": "string",
            "policyVersionId": "string"
          },
          "account": "string"
        },
        "additionalInfo": {
          "string": "string"
        }
      }
    ],
    ".reasonForNonCompliance": "string",
    "reasonForNonComplianceCode": "string"
  }
```
```json
{}
"nextToken": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>findings</td>
<td>list</td>
<td>The findings (results) of the audit.</td>
</tr>
<tr>
<td></td>
<td>member: AuditFinding</td>
<td></td>
</tr>
<tr>
<td>taskId</td>
<td>string</td>
<td>The ID of the audit that generated this result (finding)</td>
</tr>
<tr>
<td></td>
<td>length- max:40 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-]+</td>
<td></td>
</tr>
<tr>
<td>checkName</td>
<td>string</td>
<td>The audit check that generated this result.</td>
</tr>
<tr>
<td>taskStartTime</td>
<td>timestamp</td>
<td>The time the audit started.</td>
</tr>
<tr>
<td>findingTime</td>
<td>timestamp</td>
<td>The time the result (finding) was discovered.</td>
</tr>
<tr>
<td>severity</td>
<td>string</td>
<td>The severity of the result (finding).</td>
</tr>
<tr>
<td></td>
<td>enum: CRITICAL</td>
<td>HIGH</td>
</tr>
<tr>
<td>nonCompliantResource</td>
<td>NonCompliantResource</td>
<td>The resource that was found to be non-compliant with the audit check.</td>
</tr>
<tr>
<td>resourceType</td>
<td>string</td>
<td>The type of the non-compliant resource.</td>
</tr>
<tr>
<td></td>
<td>enum: DEVICE_CERTIFICATE</td>
<td>CA_CERTIFICATE</td>
</tr>
<tr>
<td>resourceId</td>
<td>ResourceIdentifier</td>
<td>Information identifying the non-compliant resource.</td>
</tr>
<tr>
<td>deviceCertificateId</td>
<td>string</td>
<td>The ID of the certificate attached to the resource.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: (0x)?[a-fA-F0-9]+</td>
<td></td>
</tr>
<tr>
<td>caCertificateId</td>
<td>string</td>
<td>The ID of the CA certificate used to authorize the certificate.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: (0x)?[a-fA-F0-9]+</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cognitoIdentityPoolId</td>
<td>string</td>
<td>The ID of the Cognito Identity Pool.</td>
</tr>
<tr>
<td>clientId</td>
<td>string</td>
<td>The client ID.</td>
</tr>
<tr>
<td>policyVersionIdentifier</td>
<td>PolicyVersionIdentifier</td>
<td>The version of the policy associated with the resource.</td>
</tr>
<tr>
<td>policyName</td>
<td>string</td>
<td>The name of the policy.</td>
</tr>
<tr>
<td>policyVersionId</td>
<td>string</td>
<td>The ID of the version of the policy associated with the resource.</td>
</tr>
<tr>
<td>account</td>
<td>string</td>
<td>The account with which the resource is associated.</td>
</tr>
<tr>
<td>additionalInfo</td>
<td>map</td>
<td>Additional information about the non-compliant resource.</td>
</tr>
<tr>
<td>relatedResources</td>
<td>list</td>
<td>The list of related resources.</td>
</tr>
<tr>
<td>resourceType</td>
<td>string</td>
<td>The type of resource.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: DEVICE_CERTIFICATE</td>
</tr>
<tr>
<td>resourceIdentifier</td>
<td>ResourceIdentifier</td>
<td>Information identifying the resource.</td>
</tr>
<tr>
<td>deviceCertificateId</td>
<td>string</td>
<td>The ID of the certificate attached to the resource.</td>
</tr>
<tr>
<td>caCertificateId</td>
<td>string</td>
<td>The ID of the CA certificate used to authorize the certificate.</td>
</tr>
<tr>
<td>cognitoIdentityPoolId</td>
<td>string</td>
<td>The ID of the Cognito Identity Pool.</td>
</tr>
<tr>
<td>clientId</td>
<td>string</td>
<td>The client ID.</td>
</tr>
</tbody>
</table>
Device Defender Detect allows you to identify unusual behavior that may indicate a compromised device by monitoring the behavior of your devices. Using a combination of cloud-side metrics (from AWS IoT) and device-side metrics (from agents you install on your devices) you can detect changes in connection patterns, devices that communicate to unauthorized or unrecognized endpoints, and changes in inbound and outbound device traffic patterns. You create security profiles, which contain
definitions of expected device behaviors, and assign them to a group of devices or to all the devices in your fleet. Device Defender Detect uses these security profiles to detect anomalies and send alerts via AWS CloudWatch metrics and AWS SNS notifications.

Device Defender Detect is capable of detecting a variety of security issues frequently found in connected devices:

- Traffic from a device to a known malicious IP address or to an unauthorized endpoint that indicates a potential malicious command and control channel.
- Anomalous traffic, such as a spike in outbound traffic, that indicates a device is participating in a DDoS.
- Devices with remote management interfaces and ports that are remotely accessible.
- A spike in the rate of messages sent to your account—so that a rogue device does not end up costing you in per-message charges.

**Use cases:**

**Measure attack surface**

You can use Device Defender Detect to measure the attack surface of your devices. For example, you can identify devices with service ports which are often the target of attack campaigns (telnet service running on ports 23/2323, SSH service running on port 22, HTTP/S services running on ports 80/443/8080/8081). While these service ports might have legitimate reasons to be used on the devices, they are also usually part of the attack surface for adversaries and carry associated risks. After Detect alerts you to the attack surface, you can either decide to minimize it (by eliminating unused network services) or run additional assessments to identify security weaknesses (for example, telnet configured with common, default or weak passwords).

**Detect device behavioral anomalies with possible security root causes**

You can use Device Defender Detect to alert you to unexpected device behavioral metrics (the number of open ports, number of connections, an unexpected open port, connections to unexpected IP addresses) which might indicate a security breach. For example, a higher than expected number of TCP connections may indicate a device is being used for a DDoS attack. A process listening on a port other than the one you expect may indicate a backdoor installed on a device for remote control. You can use Detect to probe the health of your device fleets and verify your security assumptions (for example, no device is listening on port 23 or 2323).

**Detect a mis-configured device**

A spike in the number or size of messages sent from a device to your account might indicate a mis-configured device. Such a device could increase your per-message charges. Similarly, a device with many authorization failures could require a re-configured policy.

**Concepts**

**metric**

Device Defender Detect uses metrics to detect anomalous behavior. Detect compares the reported value of a metric with the expected value you provide. These metrics can be taken from two sources: (a) cloud-side metrics, and (b) device-side metrics:

(a) Abnormal behavior on the AWS IoT network is detected by using cloud-side metrics such as the number of authorization failures, or the number or size of messages a device sends or receives via AWS IoT.

(b) Device Defender Detect can also collect, aggregate, and monitor metrics data generated by AWS IoT devices, for example, the ports a device is listening on, the number of bytes or packets sent, or the device's TCP connections.
You can use Device Defender Detect with cloud-side metrics alone. To use device-side metrics you must first deploy an agent on your AWS IoT connected devices or device gateways to collect the metrics and send them to AWS IoT. See Sending Metrics from Devices (p. 468)

A security profile defines anomalous behaviors for a group of devices (a thing group) or for all devices in your account, and specifies what actions to take when an anomaly is detected. You can create a security profile and associate it with a group of devices using the console or with AWS IoT API commands. Device Defender Detect starts recording security-related data and uses the behaviors defined in the security profile to detect anomalies in the behavior of the devices.

A behavior tells Device Defender Detect how to recognize when a device is doing something abnormal. Each behavior consists of a name, a metric, an operator, a value, and, in some cases, a time period (duration). Any device action that does not match a defined behavior statement triggers an alert.

When an anomaly is detected, an alert notification can be sent via a CloudWatch metric or an SNS notification. An alert notification is also displayed in the AWS IoT CDM console along with additional information about the alert, and a history of alerts for the device. An alert is also sent when a monitored device stops exhibiting anomalous behavior or when it had been causing an alert but stops reporting for an extended period.

### Metrics

**aws:message-byte-size**

The number of bytes in a message.

Use this metric to specify the maximum or minimum size (in bytes) of each message transmitted from a device to AWS IoT.

Source: cloud-side

Operators: less-than | less-than-equals | greater-than | greater-than-equals

Value: a non-negative integer

Units: bytes

Example:

```json
{
  "name": "Max Message Size",
  "metric": "aws:message-byte-size",
  "criteria": {
    "comparisonOperator": "less-than",
    "value": {
      "count": 1024
    }
  }
}
```
aws:num-messages-received / aws:num-messages-sent

The number of messages received or sent by a device during a given time period.

Use this metric to specify the maximum or minimum number of messages that may be sent or received between AWS IoT and each device in a given period of time.

Source: cloud-side

Operators: less-than | less-than-equals | greater-than | greater-than-equals

Value: a non-negative integer

Units: messages

Duration: a non-negative integer, valid values are 300, 600, 900, 1800 or 3600 seconds

Example:

```json
{
    "name": "Outbound message count",
    "metric": "aws:num-messages-sent",
    "criteria": {
        "comparisonOperator": "less-than",
        "value": {
            "count": 50
        },
        "durationSeconds": "300"
    }
}
```

aws:all-bytes-out

The number of outbound bytes from a device during a given time period.

Use this metric to specify the maximum or minimum amount of out-bound traffic that a device should send, measured in bytes in a given period of time.

Source: device-side

Operators: less-than | less-than-equals | greater-than | greater-than-equals

Value: a non-negative integer

Units: bytes

Duration: a non-negative integer, valid values are 300, 600, 900, 1800 or 3600 seconds

Example:

```json
{
    "name": "TCP outbound traffic",
    "metric": "aws:all-bytes-out",
    "criteria": {
        "comparisonOperator": "less-than",
        "value": {
            "count": 50
        },
        "durationSeconds": "300"
    }
}
```
aws:all-bytes-in

The number of inbound bytes to a device during a given time period.

more info (4)

Use this metric to specify the maximum or minimum amount of in-bound traffic that a device should receive, measured in bytes in a given period of time.

Source: device-side

Operators: less-than | less-than-equals | greater-than | greater-than-equals

Value: a non-negative integer

Units: bytes

Duration: a non-negative integer, valid values are 300, 600, 900, 1800 or 3600 seconds

Example:

```json
{
    "name": "TCP inbound traffic",
    "metric": "aws:all-bytes-in",
    "criteria": {
        "comparisonOperator": "less-than",
        "value": {
            "count": 4096
        },
        "durationSeconds": "300"
    }
}
```

aws:all-packets-out

The number of outbound packets from a device during a given time period.

more info (5)

Use this metric to specify the maximum or minimum amount of total outbound traffic that a device should send in a given period of time.

Source: device-side

Operators: less-than | less-than-equals | greater-than | greater-than-equals

Value: a non-negative integer
Units: packets

Duration: a non-negative integer, valid values are 300, 600, 900, 1800 or 3600 seconds

Example:

```
{
    "name": "TCP outbound traffic",
    "metric": "aws:all-packets-out",
    "criteria": {
        "comparisonOperator": "less-than",
        "value": {
            "count": 100
        },
        "durationSeconds": "300"
    }
}
```

aws:all-packets-in

The number of inbound packets to a device during a given time period.

more info (6)

Use this metric to specify the maximum or minimum amount of total inbound traffic that a device should receive in a given period of time.

Source: device-side

Operators: less-than | less-than-equals | greater-than | greater-than-equals

Value: a non-negative integer

Units: packets

Duration: a non-negative integer, valid values are 300, 600, 900, 1800 or 3600 seconds

Example:

```
{
    "name": "TCP inbound traffic",
    "metric": "aws:all-packets-in",
    "criteria": {
        "comparisonOperator": "less-than",
        "value": {
            "count": 100
        },
        "durationSeconds": "300"
    }
}
```

aws:num-authorization-failures

The number of authorization failures during a given time period.
Use this metric to specify the maximum number of authorization failures allowed for each device in a given period of time. An authorization failure occurs when a request from a device to AWS IoT is denied, for example, if a device attempts to publish to a topic for which it does not have sufficient permissions.

**Source:** cloud-side

**Unit:** failures

**Operators:** less-than | less-than-equals | greater-than | greater-than-equals

**Value:** a non-negative integer

**Units:** failures

**Duration:** a non-negative integer, valid values are 300, 600, 900, 1800 or 3600 seconds

**Example:**

```
{
    "name": "Authorization Failures",
    "metric": "aws:num-authorization-failures",
    "criteria": {
        "comparisonOperator": "less-than",
        "value": {
            "count": 5
        },
        "durationSeconds": "300"
    }
}
```

*aws:source-ip-address*

The IP address from which a device has connected to AWS IoT.

Use this metric to specify a set of whitelisted or blacklisted CIDRs from which each device must or must not connect to AWS IoT.

**Source:** cloud-side

**Operators:** in-cidr-set | not-in-cidr-set

**Values:** a list of CIDRs

**Units:** n/a

**Example:**

```
{
    "name": "Blacklisted source IPs",
    "metric": "aws:source-ip-address",
    "criteria": {
        "comparisonOperator": "not-in-cidr-set",
    }
}
```
aws:destination-ip-addresses

A set of IP destinations.

more info (9)

Use this metric to specify a set of whitelisted or blacklisted CIDRs that each device must or must not communicate with.

Source: device-side

Operators: in-cidr-set | not-in-cidr-set

Values: a list of CIDRs

Units: n/a

Example:

```json
{
  "name": "Blacklisted destination IPs",
  "metric": "aws:destination-ip-addresses",
  "criteria": {
    "comparisonOperator": "not-in-cidr-set",
    "value": {
      "cidrs": [ "12.8.0.0/16", "15.102.16.0/24" ]
    }
  }
}
```

aws:listening-tcp-ports / aws:listening-udp-ports

The TCP or UDP ports that the device is listening on.

more info (11)

Use this metric to specify a set of whitelisted or blacklisted TCP/UDP ports that each device must or must not listen on.

Source: device-side

Operators: in-port-set | not-in-port-set

Values: a list of ports

Units: n/a

Example:
aws:num-listening-tcp-ports / aws:num-listening-udp-ports

The number of TCP or UDP ports the device is listening on.

Use this metric to specify the maximum or minimum number of TCP or UDP ports that each device should listen on.

Source: device-side

Operators: less-than | less-than-equals | greater-than | greater-than-equals

Value: a non-negative integer

Units: ports

Example:

```json
{
    "name": "Max TCP Ports",
    "metric": "aws:num-listening-tcp-ports",
    "criteria": {
        "comparisonOperator": "less-than-equals",
        "value": {
            "count": 4
        }
    }
}
```

aws:num-established-tcp-connections

The number of TCP connections for a device.

Use this metric to specify the maximum or minimum number of active TCP connections that each device should have. (All TCP states)

Source: device-side

Operators: less-than | less-than-equals | greater-than | greater-than-equals

Value: a non-negative integer
Units: connections

Example:

```
{
    "name": "TCP Connection Count",
    "metric": "aws:num-established-tcp-connections",
    "criteria": {
        "comparisonOperator": "less-than",
        "value": {
            "count": 3
        }
    }
}
```

How To Use Device Defender Detect

1. You can use Device Defender Detect with just cloud-side metrics, but if you plan to use device reported metrics, you must first deploy an agent on your AWS IoT connected devices or device gateways. See Sending Metrics from Devices (p. 468).

2. Create a set of behaviors that go in your security profile. Behaviors contain metrics that specify normal behavior for a group of devices or for all devices in your account. You can find more information, including examples, in Metrics (p. 459). After you have created a set of behaviors you can validate them with ValidateSecurityProfileBehaviors (p. 516).

3. Use CreateSecurityProfile (p. 474) to create a security profile that includes your behaviors. You can have alerts sent to a target (an SNS topic) when a device violates a behavior by using the alertTargets parameter. (If you do send alerts using SNS be aware that these will count against your account's SNS limit. It is possible for a large burst of violations to exhaust your capacity.)

4. Use AttachSecurityProfile (p. 472) to attach the security profile to a group of devices (a thing group) or to all the devices in your account. Device Defender Detect will begin checking for abnormal behavior and will send alerts if any behavior violations are detected.

To attach a security profile to a group of devices, you must specify the ARN of the thing group which contains them. A thing group ARN has the following format:

```
arn:aws:iot:<region>:<accountid>:thinggroup/<thing-group-name>
```

To attach a security profile to all of the devices in an account, you must specify an ARN with the following format:

```
arn:aws:iot:<region>:<accountid>:all/things
```

5. You can also keep track of violations with ListActiveViolations (p. 488) which allows you to see what violations have been detected for a given security profile or target device.

   Use ListViolationEvents (p. 502) to see what violations have been detected during a specified time period. You can filter these results by a given security profile or device.

6. If you need to review the security profiles you have set up and the devices that are being monitored, use ListSecurityProfiles (p. 493), ListSecurityProfilesForTarget (p. 496), and ListTargetsForSecurityProfile (p. 499).

   You can get more details about a particular security profile with DescribeSecurityProfile (p. 481).

7. To make changes to a security profile, use UpdateSecurityProfile (p. 508). You may detach it from an account or target thing group with DetachSecurityProfile (p. 486) or delete a security profile with DeleteSecurityProfile (p. 479).
Permissions

This section contains information on how to set up the AWS IAM roles and policies required to manage Device Defender Detect. For more information on AWS IAM, see the AWS Identity and Access Management User Guide.

Give Device Defender Detect permission to publish alerts to an SNS topic.

If you use the alertTargets parameter in CreateSecurityProfile (p. 474), you must specify an IAM Role with two policies, a permissions policy and a trust policy. The permissions policy grants permission to Device Defender to publish notifications to your SNS topic. The trust policy grants Device Defender permission to assume the required role.

permissions policy

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sns:Publish"
      ],
      "Resource": [
        "arn:aws:sns:region:account-id:your-topic-name"
      ]
    }
  ]
}
```

trust policy

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "iot.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Service Limits

- The maximum number of security profiles per target (thing group or user account) is 5.
- The maximum number of behaviors per security profile is 100.
- The maximum number of value elements (counts, IP addresses, ports) per security profile is 1000.
- Device metric reporting is throttled to one metric per 5 minutes per device (a device may not report more than one metric every 5 minutes).
- Device Defender Detect violations are stored for 90 days after they have been generated.
Sending Metrics from Devices

Device Defender Detect can collect, aggregate, and monitor metrics data generated by AWS IoT devices to identify devices that are exhibiting abnormal behavior. This section contains information on how to send metrics from a device to AWS IoT Device Defender.

You must securely deploy an agent on your AWS IoT connected devices or device gateways to collect device-side metrics. Device Defender provides a sample agent to use as an example when creating your own. Alternatively, you can provide device-side metrics to Device Defender in a pre-determined format and frequency. If you are unable to provide device metrics in one of these ways, you can still get limited functionality based on cloud-side metrics.

Please note the following:

- A sample device metric reporting agent is currently available in Python on GitHub at https://github.com/aws-samples/aws-iot-device-defender-agent-sdk-python/tree/master/samples/greengrass/greengrass_core_metrics_agent.
- In order to report metrics, a device must be registered as a thing in AWS IoT.
- A device should, generally, send metrics once every 5 minutes. Device metric reporting is throttled to one metric per minute per device (a device may not report more than one metric per minute).
- Devices must report current metrics; historical metrics reporting is not supported.

Device Metrics Document Specification

Overall Structure:

<table>
<thead>
<tr>
<th>Long Name</th>
<th>Short Name</th>
<th>Required</th>
<th>Type</th>
<th>Constraints</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>header</td>
<td>hed</td>
<td>Y</td>
<td>Object</td>
<td></td>
<td>Complete block required for well-formed report.</td>
</tr>
<tr>
<td>metrics</td>
<td>met</td>
<td>Y</td>
<td>Object</td>
<td></td>
<td>Complete block required for well-formed report.</td>
</tr>
</tbody>
</table>

Header Block:

<table>
<thead>
<tr>
<th>Long Name</th>
<th>Short Name</th>
<th>Required</th>
<th>Type</th>
<th>Constraints</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>report_id</td>
<td>rid</td>
<td>Y</td>
<td>Integer</td>
<td></td>
<td>Monotonically increasing value, epoch timestamp recommended</td>
</tr>
<tr>
<td>version</td>
<td>v</td>
<td>Y</td>
<td>String</td>
<td>Major.Minor</td>
<td>minor increments with addition of field, major increments if metrics removed</td>
</tr>
</tbody>
</table>
**Metrics Block:**

**TCP Connections:**

<table>
<thead>
<tr>
<th>Long Name</th>
<th>Short Name</th>
<th>Parent Element</th>
<th>Required</th>
<th>Type</th>
<th>Constraints</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp_connections</td>
<td>tc</td>
<td>metrics</td>
<td>N</td>
<td>Object</td>
<td></td>
<td></td>
</tr>
<tr>
<td>established_connections</td>
<td>ec</td>
<td>tcp_connections</td>
<td>N</td>
<td>List&lt;Connection&gt;</td>
<td></td>
<td>ESTABLISHED TCP State</td>
</tr>
<tr>
<td>connections</td>
<td>cs</td>
<td>established_connections</td>
<td>Y</td>
<td>Number</td>
<td>ip:port</td>
<td>ip can be ipv6 or ipv4</td>
</tr>
<tr>
<td>remote_addr</td>
<td>rad</td>
<td>connections</td>
<td>N</td>
<td>Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>local_port</td>
<td>lp</td>
<td>connections</td>
<td>N</td>
<td>Number</td>
<td>&gt;= 0</td>
<td></td>
</tr>
<tr>
<td>local_interface</td>
<td>li</td>
<td>connections</td>
<td>N</td>
<td>String</td>
<td></td>
<td>interface name</td>
</tr>
<tr>
<td>total</td>
<td>t</td>
<td>established_connections</td>
<td>N</td>
<td>Number</td>
<td>&gt;= 0</td>
<td>Number of established connections</td>
</tr>
</tbody>
</table>

**Listening TCP Ports:**

<table>
<thead>
<tr>
<th>Long Name</th>
<th>Short Name</th>
<th>Parent Element</th>
<th>Required</th>
<th>Type</th>
<th>Constraints</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>listening_tcp_ports</td>
<td>pts</td>
<td>metrics</td>
<td>N</td>
<td>Object</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ports</td>
<td>pts</td>
<td>listening_tcp_ports</td>
<td>N</td>
<td>List&lt;Port&gt;</td>
<td>&gt; 0</td>
<td>ports should be numbers &gt; 0</td>
</tr>
<tr>
<td>port</td>
<td>pt</td>
<td>ports</td>
<td>N</td>
<td>Number</td>
<td>&gt; 0</td>
<td></td>
</tr>
<tr>
<td>interface</td>
<td>if</td>
<td>ports</td>
<td>N</td>
<td>String</td>
<td></td>
<td>interface name</td>
</tr>
<tr>
<td>total</td>
<td>t</td>
<td>listening_tcp_ports</td>
<td>N</td>
<td>Number</td>
<td>&gt;= 0</td>
<td></td>
</tr>
</tbody>
</table>

**Listening UDP Ports:**

<table>
<thead>
<tr>
<th>Long Name</th>
<th>Short Name</th>
<th>Parent Element</th>
<th>Required</th>
<th>Type</th>
<th>Constraints</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>listening_udp_ports</td>
<td>pts</td>
<td>metrics</td>
<td>N</td>
<td>Object</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ports</td>
<td>pts</td>
<td>listening_udp_ports</td>
<td>N</td>
<td>List&lt;Port&gt;</td>
<td>&gt; 0</td>
<td>ports should be numbers &gt; 0</td>
</tr>
<tr>
<td>port</td>
<td>pt</td>
<td>ports</td>
<td>N</td>
<td>Number</td>
<td>&gt; 0</td>
<td></td>
</tr>
<tr>
<td>interface</td>
<td>if</td>
<td>ports</td>
<td>N</td>
<td>String</td>
<td></td>
<td>interface name</td>
</tr>
</tbody>
</table>
Long Name | Short Name | Parent Element | Required | Type | Constraints | Notes
---|---|---|---|---|---|---
total | t | listening_udp_ports | N | Number | >= 0 | 

### Network Stats:

<table>
<thead>
<tr>
<th>Long Name</th>
<th>Short Name</th>
<th>Parent Element</th>
<th>Required</th>
<th>Type</th>
<th>Constraints</th>
<th>Notes</th>
</tr>
</thead>
</table>
network_stats | ns | metrics | N | Object | | |
bytes_in | bi | network_stats | N | Number | Delta Metric, >= 0 | |
bytes_out | bo | network_stats | N | Number | Delta Metric, >= 0 | |
packets_in | pi | network_stats | N | Number | Delta Metric, >= 0 | |
packets_out | po | network_stats | N | Number | Delta Metric, >= 0 | |

Example JSON structure using long names:

```json
{
    "header": {
        "report_id": 1530304554,
        "version": "1.0"
    },
    "metrics": {
        "listening_tcp_ports": {
            "ports": [
                {
                    "interface": "eth0",
                    "port": 24800
                },
                {
                    "interface": "eth0",
                    "port": 22
                },
                {
                    "interface": "eth0",
                    "port": 53
                }
            ],
            "total": 3
        },
        "listening_udp_ports": {
            "ports": [
                {
                    "interface": "eth0",
                    "port": 5353
                },
                {
                    "interface": "eth0",
                    "port": 67
                }
            ]
        }
    }
}
```
Example JSON structure using short names:

```
{
  "hed": {
    "rid": 1530305228,
    "v": "1.0"
  },
  "met": {
    "tp": {
      "pts": [
        {
          "if": "eth0",
          "pt": 24800
        },
        {
          "if": "eth0",
          "pt": 22
        },
        {
          "if": "eth0",
          "pt": 53
        }
      ],
      "t": 3
    },
    "up": {
      "pts": [
        {
          "if": "eth0",
          "pt": 5353
        },
        {
          "if": "eth0",
          "pt": 67
        }
      ],
      "t": 2
    }
  }
}
```
**Detect Commands**

**AttachSecurityProfile**

Associates a Device Defender security profile with a thing group or with this account. Each thing group or account can have up to five security profiles associated with it.

[https](#)

**Request syntax:**

PUT /security-profiles/{securityProfileName}/targets?securityProfileTargetArn={securityProfileTargetArn}

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>yes</td>
<td>The security profile that is attached.</td>
</tr>
<tr>
<td>securityProfileTargetArn</td>
<td>SecurityProfileTargetArn</td>
<td>yes</td>
<td>The ARN of the target (thing group) to which the security profile is attached.</td>
</tr>
</tbody>
</table>

**Errors:**
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

LimitExceededException

A limit has been exceeded.

HTTP response code: 410

VersionConflictException

An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

HTTP response code: 409

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```bash
aws iot attach-security-profile
    --security-profile-name <value> \
    --security-profile-target-arn <value> \
    [--cli-input-json <value>] \n    [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
    "securityProfileName": "string",
    "securityProfileTargetArn": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The security profile that is attached.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td>pattern: [a-zA-Z0-9_:-]+</td>
</tr>
</tbody>
</table>
CreateSecurityProfile

Creates a Device Defender security profile.

https

Request syntax:

```json
POST /security-profiles/securityProfileName
Content-type: application/json

{
  "securityProfileDescription": "string",
  "behaviors": [
    {
      "name": "string",
      "metric": "string",
      "criteria": {
        "comparisonOperator": "string",
        "value": {
          474
        }
      }
    }
  ]
}
```
CreateSecurityProfile

```
"count": "long",
"cidrs": [
  "string"
],
"ports": [
  "integer"
],
"durationSeconds": "integer"
},
"alertTargets": {
  "string": {
    "alertTargetArn": "string",
    "roleArn": "string"
  }
}
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>yes</td>
<td>The name you are giving to the security profile.</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileDescription</td>
<td>SecurityProfileDescription</td>
<td>no</td>
<td>A description of the security profile.</td>
</tr>
<tr>
<td>behaviors</td>
<td>Behaviors</td>
<td>yes</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td>alertTargets</td>
<td>AlertTargets</td>
<td>no</td>
<td>Specifies the destinations to which alerts are sent. (Alerts are always sent to the console.) Alerts are generated when a device (thing) violates a behavior.</td>
</tr>
</tbody>
</table>

**Response syntax:**

```
Content-type: application/json

{
  "securityProfileName": "string",
  "securityProfileArn": "string"
}
```
Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>no</td>
<td>The name you gave to the security profile.</td>
</tr>
<tr>
<td>securityProfileArn</td>
<td>SecurityProfileArn</td>
<td>no</td>
<td>The ARN of the security profile.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceAlreadyExistsException

The resource already exists.

HTTP response code: 409

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot create-security-profile
   --security-profile-name <value> \
   [--security-profile-description <value>] \
   --behaviors <value> \ 
   [--alert-targets <value>] \ 
   [--cli-input-json <value>] \ 
   [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
   "securityProfileName": "string",
   "securityProfileDescription": "string",
   "behaviors": [
      {
         "name": "string",
         "metric": "string",
         "criteria": {
            "comparisonOperator": "string",
            "value": {
            ...
```
"count": "long",
"cidrs": [
  "string"
],
"ports": [
  "integer"
],
"durationSeconds": "integer"
}
}
"alertTargets": {
  "string": {
    "alertTargetArn": "string",
    "roleArn": "string"
  }
}
}
"cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name you are giving to the security profile.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:._-]+</td>
<td></td>
</tr>
<tr>
<td>securityProfileDescription</td>
<td>string</td>
<td>A description of the security profile.</td>
</tr>
<tr>
<td></td>
<td>length- max:1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [\p{Graph}]*</td>
<td></td>
</tr>
<tr>
<td>behaviors</td>
<td>list</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td></td>
<td>member: Behavior</td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the behavior.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:._-]+</td>
<td></td>
</tr>
<tr>
<td>metric</td>
<td>string</td>
<td>What is measured by the behavior.</td>
</tr>
<tr>
<td>criteria</td>
<td>BehaviorCriteria</td>
<td>The criteria that determine if a device is behaving normally in regard to the metric.</td>
</tr>
<tr>
<td>comparisonOperator</td>
<td>string</td>
<td>The operator that relates the thing measured (metric) to the criteria (value).</td>
</tr>
<tr>
<td></td>
<td>enum: less-than</td>
<td></td>
</tr>
<tr>
<td></td>
<td>less-than-equals</td>
<td></td>
</tr>
<tr>
<td></td>
<td>greater-than</td>
<td></td>
</tr>
<tr>
<td></td>
<td>greater-than-equals</td>
<td></td>
</tr>
<tr>
<td></td>
<td>in-cidr-set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>not-in-cidr-set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>in-port-set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>not-in-port-set</td>
<td></td>
</tr>
</tbody>
</table>
### Name | Type | Description
--- | --- | ---
value | MetricValue | The value to be compared with the metric.  

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| count | long | If the comparisonOperator calls for a numeric value, use this to specify that numeric value to be compared with the metric.  

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| cidrs | list | If the comparisonOperator calls for a set of CIDRs, use this to specify that set to be compared with the metric.  

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| ports | list | If the comparisonOperator calls for a set of ports, use this to specify that set to be compared with the metric.  

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| durationSeconds | integer | Use this to specify the period of time over which the behavior is evaluated, for those criteria which have a time dimension (for example, num_messages_sent).  

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| alertTargets | map | Specifies the destinations to which alerts are sent. (Alerts are always sent to the console.) Alerts are generated when a device (thing) violates a behavior.  

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| alertTargetArn | string | The ARN of the notification target to which alerts are sent.  

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| roleArn | string | The ARN of the role that grants permission to send alerts to the notification target.  

### Output:

```json
{
  "securityProfileName": "string",
  "securityProfileArn": "string"
}
```

### cli output fields:

### Name | Type | Description
--- | --- | ---
securityProfileName | string | The name you gave to the security profile.  

---

478
DeleteSecurityProfile

Deletes a Device Defender security profile.

https

Request syntax:

```
DELETE /security-profiles/securityProfileName?expectedVersion=expectedVersion
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>yes</td>
<td>The name of the security profile to be deleted.</td>
</tr>
<tr>
<td>expectedVersion</td>
<td>OptionalVersion</td>
<td>no</td>
<td>The expected version of the security profile. A new version is generated whenever the security profile is updated. If you specify a value that is different than the actual version, a VersionConflictException is thrown.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceAlreadyExistsException

The resource already exists.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

VersionConflictException

An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

HTTP response code: 409

cli

Synopsis:

aws iot delete-security-profile \
   --security-profile-name <value> \
   [--expected-version <value>] \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]

cli-input-json format:

{
   "securityProfileName": "string",
   "expectedVersion": "long"
}

ci-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name of the security profile to be deleted.</td>
</tr>
<tr>
<td></td>
<td>length-</td>
<td>max:128 min:1 pattern: [a-zA-Z0-9-_]+</td>
</tr>
<tr>
<td>expectedVersion</td>
<td>long</td>
<td>The expected version of the security profile. A new version is generated whenever the security profile is updated. If you specify a value that is different than the actual version, a VersionConflictException is thrown.</td>
</tr>
</tbody>
</table>
DescribeSecurityProfile

Gets information about a Device Defender security profile.

https

Request syntax:

GET /security-profiles/securityProfileName

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>yes</td>
<td>The name of the security profile whose information you want to get.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{
  "securityProfileName": "string",
  "securityProfileArn": "string",
  "securityProfileDescription": "string",
  "behaviors": [
    {
      "name": "string",
      "metric": "string",
      "criteria": {
        "comparisonOperator": "string",
        "value": {
          "comparisonType": "string",
          "value": "string"
        }
      }
    }
  ]
}
"count": "long",
"cidrs": [
    "string"
],
"ports": [
    "integer"
],
"durationSeconds": "integer"
},
"alertTargets": {
    "string": {
        "alertTargetArn": "string",
        "roleArn": "string"
    }
},
"version": "long",
"creationDate": "timestamp",
"lastModifiedDate": "timestamp"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>no</td>
<td>The name of the security profile.</td>
</tr>
<tr>
<td>securityProfileArn</td>
<td>SecurityProfileArn</td>
<td>no</td>
<td>The ARN of the security profile.</td>
</tr>
<tr>
<td>securityProfileDescription</td>
<td>SecurityProfileDescription</td>
<td>no</td>
<td>A description of the security profile (associated with the security profile when it was created or updated).</td>
</tr>
<tr>
<td>behaviors</td>
<td>Behaviors</td>
<td>no</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td>alertTargets</td>
<td>AlertTargets</td>
<td>no</td>
<td>Where the alerts are sent. (Alerts are always sent to the console.)</td>
</tr>
<tr>
<td>version</td>
<td>Version</td>
<td>no</td>
<td>The version of the security profile. A new version is generated whenever the security profile is updated.</td>
</tr>
<tr>
<td>creationDate</td>
<td>Timestamp</td>
<td>no</td>
<td>The time the security profile was created.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>Timestamp</td>
<td>no</td>
<td>The time the security profile was last modified.</td>
</tr>
</tbody>
</table>
Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an
UpdateJobExecution request contains invalid status details. The message contains details about the
error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

aws iot  describe-security-profile \
  --security-profile-name <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]

cli-input-json format:

{
  "securityProfileName": "string"
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name of the security profile whose information you want to get.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>length- max:128 min:1</th>
</tr>
</thead>
<tbody>
<tr>
<td>pattern: [a-zA-Z0-9_:-]+</td>
</tr>
</tbody>
</table>

Output:

```json
{
  "securityProfileName": "string",
  "securityProfileArn": "string",
  "securityProfileDescription": "string",
  "behaviors": [ 
    
```
"name": "string",
"metric": "string",
"criteria": {
    "comparisonOperator": "string",
    "value": {
        "count": "long",
        "cidrs": [
            "string"
        ],
        "ports": [
            "integer"
        ],
        "durationSeconds": "integer"
    }
},
"alertTargets": {
    "string": {
        "alertTargetArn": "string",
        "roleArn": "string"
    }
},
"version": "long",
"creationDate": "timestamp",
"lastModifiedDate": "timestamp"
}

### cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name of the security profile.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>securityProfileArn</td>
<td>string</td>
<td>The ARN of the security profile.</td>
</tr>
<tr>
<td>securityProfileDescription</td>
<td>string</td>
<td>A description of the security profile (associated with the security profile when it was created or updated).</td>
</tr>
<tr>
<td></td>
<td>length- max:1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [\p{Graph}]*</td>
<td></td>
</tr>
<tr>
<td>behaviors</td>
<td>list</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td></td>
<td>member: Behavior</td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the behavior.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>metric</td>
<td>string</td>
<td>What is measured by the behavior.</td>
</tr>
<tr>
<td>criteria</td>
<td>BehaviorCriteria</td>
<td>The criteria that determine if a device is behaving normally in regard to the metric.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>comparisonOperator</td>
<td>string</td>
<td>The operator that relates the thing measured (metric) to the criteria (value).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: less-than</td>
</tr>
<tr>
<td>value</td>
<td>MetricValue</td>
<td>The value to be compared with the metric.</td>
</tr>
<tr>
<td>count</td>
<td>long</td>
<td>If the comparisonOperator calls for a numeric value, use this to specify that numeric value to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>range- min:0</td>
</tr>
<tr>
<td>cidrs</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of CIDRs, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>list</td>
<td>member: Cidr</td>
</tr>
<tr>
<td>ports</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of ports, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>list</td>
<td>member: Port</td>
</tr>
<tr>
<td>durationSeconds</td>
<td>integer</td>
<td>Use this to specify the period of time over which the behavior is evaluated, for those criteria which have a time dimension (for example, NUM_MESSAGES_SENT).</td>
</tr>
<tr>
<td>alertTargets</td>
<td>map</td>
<td>Where the alerts are sent. (Alerts are always sent to the console.)</td>
</tr>
<tr>
<td>alertTargetArn</td>
<td>string</td>
<td>The ARN of the notification target to which alerts are sent.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants permission to send alerts to the notification target.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>length- max:2048 min:20</td>
</tr>
<tr>
<td>version</td>
<td>long</td>
<td>The version of the security profile. A new version is generated whenever the security profile is updated.</td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The time the security profile was created.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>timestamp</td>
<td>The time the security profile was last modified.</td>
</tr>
</tbody>
</table>
Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceNotFoundException

The specified resource does not exist.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

DetachSecurityProfile

Disassociates a Device Defender security profile from a thing group or from this account.

https

Request syntax:

DELETE /security-profiles/securityProfileName/targets?
securityProfileTargetArn=securityProfileTargetArn

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>yes</td>
<td>The security profile that is detached.</td>
</tr>
<tr>
<td>securityProfileTargetArn</td>
<td>SecurityProfileTargetArn</td>
<td>yes</td>
<td>The ARN of the thing group from which the security profile is detached.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.
HTTP response code: 429
InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

cli

Synopsis:

```
aws iot  detach-security-profile \
   --security-profile-name <value> \
   --security-profile-target-arn <value> \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "securityProfileName": "string",
   "securityProfileTargetArn": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The security profile that is detached.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>securityProfileTargetArn</td>
<td>string</td>
<td>The ARN of the thing group from which the security profile is detached.</td>
</tr>
</tbody>
</table>

Output:
None

Errors:

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceNotFoundException
The specified resource does not exist.

ThrottlingException
The rate exceeds the limit.

InternalFailureException
An unexpected error has occurred.
ListActiveViolations

Lists the active violations for a given Device Defender security profile.

https

Request syntax:

```
GET /active-violations?
maxResults=maxResults&nextToken=nextToken&thingName=thingName&securityProfileName=securityProfileName
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>no</td>
<td>The name of the thing whose active violations are listed.</td>
</tr>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>no</td>
<td>The name of the Device Defender security profile for which violations are listed.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>

Response syntax:

```
Content-type: application/json
{
  "activeViolations": [
    {
      "violationId": "string",
      "thingName": "string",
      "securityProfileName": "string",
      "behavior": {
        "name": "string",
        "metric": "string",
        "criteria": {
          "comparisonOperator": "string",
          "value": {
            "count": "long",
            "cidrs": ["string"]
          },
          "ports": [
            "integer"
          ],
          "durationSeconds": "integer"
        }
      },
      "lastViolationValue": {
```

488
"count": "long",
"cidrs": [
  "string"
],
"ports": [
  "integer"
],
"lastViolationTime": "timestamp",
"violationStartTimestamp": "timestamp"
],
"nextToken": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>activeViolations</td>
<td>ActiveViolations</td>
<td>no</td>
<td>The list of active violations.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token that can be used to retrieve the next set of results, or null if</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

ci

Synopsis:

```
aws iot list-active-violations \
    [--thing-name <value>] \
    [--security-profile-name <value>] \
```
**ListActiveViolations**

```
[--next-token <value>] \\n[--max-results <value>] \\n[--cli-input-json <value>] \\n[--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
    "thingName": "string",
    "securityProfileName": "string",
    "nextToken": "string",
    "maxResults": "integer"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing whose active violations are listed.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name of the Device Defender security profile for which violations are listed.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td></td>
<td>range- max:250 min:1</td>
<td></td>
</tr>
</tbody>
</table>

**Output:**

```json
{
    "activeViolations": [
        {
            "violationId": "string",
            "thingName": "string",
            "securityProfileName": "string",
            "behavior": {
                "name": "string",
                "metric": "string",
                "criteria": {
                    "comparisonOperator": "string",
                    "value": {
                        "count": "long",
                        "cidsrs": [
                            "string"
                        ],
                        "ports": [
                            "integer"
                        ]
                    },
                    "durationSeconds": "integer"
                }
            }
        }
    ]
}
```
AWS IoT Developer Guide
ListActiveViolations

},
"lastViolationValue": {
  "count": "long",
  "cids": [
    "string"
  ],
  "ports": [
    "integer"
  ],
  "lastViolationTime": "timestamp",
  "violationStartTime": "timestamp"
},
"nextToken": "string"

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>activeViolations</td>
<td>list</td>
<td>The list of active violations.</td>
</tr>
<tr>
<td></td>
<td>member: ActiveViolation</td>
<td></td>
</tr>
<tr>
<td>violationId</td>
<td>string</td>
<td>The ID of the active violation.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-]+</td>
<td></td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing responsible for the active violation.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_:-]+</td>
<td></td>
</tr>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The security profile whose behavior is in violation.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_:-]+</td>
<td></td>
</tr>
<tr>
<td>behavior</td>
<td>Behavior</td>
<td>The behavior which is being violated.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the behavior.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_:-]+</td>
<td></td>
</tr>
<tr>
<td>metric</td>
<td>string</td>
<td>What is measured by the behavior.</td>
</tr>
<tr>
<td>criteria</td>
<td>BehaviorCriteria</td>
<td>The criteria that determine if a device is behaving normally in regard to the metric.</td>
</tr>
<tr>
<td>comparisonOperator</td>
<td>string</td>
<td>The operator that relates the thing measured (metric) to the criteria (value).</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>value</td>
<td>MetricValue</td>
<td>The value to be compared with the metric.</td>
</tr>
<tr>
<td>count</td>
<td>long</td>
<td>If the <code>comparisonOperator</code> calls for a numeric value, use this to specify that numeric value to be compared with the metric.</td>
</tr>
<tr>
<td>cidrs</td>
<td>list</td>
<td>If the <code>comparisonOperator</code> calls for a set of CIDRs, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>ports</td>
<td>list</td>
<td>If the <code>comparisonOperator</code> calls for a set of ports, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>durationSeconds</td>
<td>integer</td>
<td>Use this to specify the period of time over which the behavior is evaluated, for those criteria which have a time dimension (for example, <code>NUM_MESSAGES_SENT</code>).</td>
</tr>
<tr>
<td>lastViolationValue</td>
<td>MetricValue</td>
<td>The value of the metric (the measurement) which caused the most recent violation.</td>
</tr>
<tr>
<td>count</td>
<td>long</td>
<td>If the <code>comparisonOperator</code> calls for a numeric value, use this to specify that numeric value to be compared with the metric.</td>
</tr>
<tr>
<td>cidrs</td>
<td>list</td>
<td>If the <code>comparisonOperator</code> calls for a set of CIDRs, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>ports</td>
<td>list</td>
<td>If the <code>comparisonOperator</code> calls for a set of ports, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>lastViolationTime</td>
<td>timestamp</td>
<td>The time the most recent violation occurred.</td>
</tr>
<tr>
<td>violationStartTime</td>
<td>timestamp</td>
<td>The time the violation started.</td>
</tr>
</tbody>
</table>
ListSecurityProfiles

Lists the Device Defender security profiles you have created. You can use filters to list only those security profiles associated with a thing group or only those associated with your account.

https

Request syntax:

GET /security-profiles?maxResults=maxResults&nextToken=nextToken

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{

"securityProfileIdentifiers": [ 
    { 
        "name": "string",
        "arn": "string"
    }
],
"nextToken": "string"

### Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileIdentifiers</td>
<td>SecurityProfileIdentifiers</td>
<td>no</td>
<td>A list of security profile identifiers (names and ARNs).</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

### Errors:

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

### Synopsis:

```bash
cli
aws iot list-security-profiles \       
    [--next-token <value>] \       
    [--max-results <value>] \       
    [--cli-input-json <value>] \   
    [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
```
"nextToken": "string",
"maxResults": "integer"
}

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time. range: max:250 min:1</td>
</tr>
</tbody>
</table>

Output:

```json
{
  "securityProfileIdentifiers": [
    {
      "name": "string",
      "arn": "string"
    }
  ],
  "nextToken": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileIdentifiers</td>
<td>list</td>
<td>A list of security profile identifiers (names and ARNs). member: SecurityProfileIdentifier java class: java.util.List</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the security profile. length: max:128 min:1 pattern: [a-zA-Z0-9-_]+</td>
</tr>
<tr>
<td>arn</td>
<td>string</td>
<td>The ARN of the security profile.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

**Errors:**

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

ListSecurityProfilesForTarget

Lists the Device Defender security profiles attached to a target (thing group).

https

Request syntax:

GET /security-profiles-for-target?
maxResults=\(maxResults\)&nextToken=nextToken&recursive=recursive&securityProfileTargetArn=securityProfileTargetArn

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td>recursive</td>
<td>Recursive</td>
<td>no</td>
<td>If true, return child groups as well.</td>
</tr>
<tr>
<td>securityProfileTargetArn</td>
<td>SecurityProfileTargetArn</td>
<td>yes</td>
<td>The ARN of the target (thing group) whose attached security profiles you want to get.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```json
{
   "securityProfileTargetMappings": [
      {
         "securityProfileIdentifier": {
            "name": "string",
            "arn": "string"
         },
         "target": {
            "arn": "string"
         }
      },
      "nextToken": "string"
   }
}
```
Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileTargetMappings</td>
<td>SecurityProfileTargetMappings</td>
<td>no</td>
<td>A list of security profiles and their associated targets.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

cli

Synopsis:

```
aws iot list-security-profiles-for-target \
   [--next-token <value>] \
   [--max-results <value>] \
   [--recursive | --no-recursive] \ 
   --security-profile-target-arn <value> \
   [--cli-input-json <value>] \ 
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "nextToken": "string",
   "maxResults": "integer",
   "recursive": "boolean",
```
"securityProfileTargetArn": "string"
}

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td></td>
<td>range:</td>
<td>max:250 min:1</td>
</tr>
<tr>
<td>recursive</td>
<td>boolean</td>
<td>If true, return child groups as well.</td>
</tr>
<tr>
<td>securityProfileTargetArn</td>
<td>string</td>
<td>The ARN of the target (thing group) whose attached security profiles you want to get.</td>
</tr>
</tbody>
</table>

Output:

```json
{
  "securityProfileTargetMappings": [
    {
      "securityProfileIdentifier": {
        "name": "string",
        "arn": "string"
      },
      "target": {
        "arn": "string"
      }
    },
    {"nextToken": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileTargetMappings</td>
<td>list</td>
<td>A list of security profiles and their associated targets.</td>
</tr>
<tr>
<td></td>
<td>member:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SecurityProfileTargetMapping</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>securityProfileIdentifier</td>
<td>SecurityProfileIdentifier</td>
<td>Information that identifies the security profile.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the security profile.</td>
</tr>
<tr>
<td></td>
<td>length: max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9_:.-]+</td>
<td></td>
</tr>
<tr>
<td>arn</td>
<td>string</td>
<td>The ARN of the security profile.</td>
</tr>
</tbody>
</table>
ListTargetsForSecurityProfile

Lists the targets (thing groups) associated with a given Device Defender security profile.

**Request syntax:**

```
GET /security-profiles/securityProfileName/targets?
maxResults=maxResults&nextToken=nextToken
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>yes</td>
<td>The security profile.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>

**Response syntax:**

- **Name**
- **Type**
- **Description**

### Errors:

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ThrottlingException**
  
  The rate exceeds the limit.

- **InternalFailureException**
  
  An unexpected error has occurred.

- **ResourceNotFoundException**
  
  The specified resource does not exist.
Content-type: application/json
{
  "securityProfileTargets": [
    {
      "arn": "string"
    },
    "nextToken": "string"
  ]
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileTargets</td>
<td>SecurityProfileTargets</td>
<td>no</td>
<td>The thing groups to which the security profile is attached.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

aws iot list-targets-for-security-profile \
ListTargetsForSecurityProfile

```
--security-profile-name <value> \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

**cli-input-json format:**

```
{
  "securityProfileName": "string",
  "nextToken": "string",
  "maxResults": "integer"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The security profile.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td></td>
<td>range- max:250 min:1</td>
<td></td>
</tr>
</tbody>
</table>

**Output:**

```
{
  "securityProfileTargets": [
    {
      "arn": "string"
    },
    "nextToken": "string"
  ]
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileTargets</td>
<td>list member: SecurityProfileTarget</td>
<td>The thing groups to which the security profile is attached.</td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>arn</td>
<td>string</td>
<td>The ARN of the security profile.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>
Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceNotFoundException

The specified resource does not exist.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

ListViolationEvents

Lists the Device Defender security profile violations discovered during the given time period. You can use filters to limit the results to those alerts issued for a particular security profile, behavior or thing (device).

https

Request syntax:

GET /violation-events?
maxResults=maxResults&nextToken=nextToken&startTime=startTime&endTime=endTime&thingName=thingName&securityProfileName=securityProfileName

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startTime</td>
<td>Timestamp</td>
<td>yes</td>
<td>The start time for the alerts to be listed.</td>
</tr>
<tr>
<td>endTime</td>
<td>Timestamp</td>
<td>yes</td>
<td>The end time for the alerts to be listed.</td>
</tr>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>no</td>
<td>A filter to limit results to those alerts caused by the specified thing.</td>
</tr>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>no</td>
<td>A filter to limit results to those alerts generated by the specified security profile.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>
Response syntax:

```json
Content-type: application/json
{
  "violationEvents": [
    {
      "violationId": "string",
      "thingName": "string",
      "securityProfileName": "string",
      "behavior": {
        "name": "string",
        "metric": "string",
        "criteria": {
          "comparisonOperator": "string",
          "value": {
            "count": "long",
            "cidrs": [
              "string"
            ],
            "ports": [
              "integer"
            ]
          },
          "durationSeconds": "integer"
        }
      },
      "metricValue": {
        "count": "long",
        "cidrs": [
          "string"
        ],
        "ports": [
          "integer"
        ]
      },
      "violationEventType": "string",
      "violationEventTime": "timestamp"
    }
  ],
  "nextToken": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>violationEvents</td>
<td>ViolationEvents</td>
<td>no</td>
<td>The security profile violation alerts issued for this account during the given time frame, potentially filtered by security profile, behavior violated, or thing (device) violating.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>
Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot list-violation-events 
  --start-time <value> 
  --end-time <value> 
  [--thing-name <value>]  
  [--security-profile-name <value>] 
  [--next-token <value>] 
  [--max-results <value>]  
  [--cli-input-json <value>] 
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "startTime": "timestamp",
  "endTime": "timestamp",
  "thingName": "string",
  "securityProfileName": "string",
  "nextToken": "string",
  "maxResults": "integer"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startTime</td>
<td>timestamp</td>
<td>The start time for the alerts to be listed.</td>
</tr>
<tr>
<td>endTime</td>
<td>timestamp</td>
<td>The end time for the alerts to be listed.</td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>A filter to limit results to those alerts caused by the specified thing.</td>
</tr>
</tbody>
</table>

- **thingName**: string, length- max:128 min:1 pattern: [a-zA-Z0-9-_]+
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>A filter to limit results to those alerts generated by the specified security profile.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>

Output:
```json
{
  "violationEvents": [
    {
      "violationId": "string",
      "thingName": "string",
      "securityProfileName": "string",
      "behavior": {
        "name": "string",
        "metric": "string",
        "criteria": {
          "comparisonOperator": "string",
          "value": {
            "count": "long",
            "cidsrs": [
              "string"
            ],
            "ports": [
              "integer"
            ]
          },
          "durationSeconds": "integer"
        }
      },
      "metricValue": {
        "count": "long",
        "cidsrs": [
          "string"
        ],
        "ports": [
          "integer"
        ],
        "violationEventType": "string",
        "violationEventTime": "timestamp"
      }
    }
  ],
  "nextToken": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>violationEvents</td>
<td>list</td>
<td>The security profile violation alerts issued for this account.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>violationId</td>
<td>string</td>
<td>The ID of the violation event.</td>
</tr>
<tr>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_:]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing responsible for the violation event.</td>
</tr>
<tr>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_:]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name of the security profile whose behavior was violated.</td>
</tr>
<tr>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_:]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>behavior</td>
<td>Behavior</td>
<td>The behavior which was violated.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the behavior.</td>
</tr>
<tr>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_:]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>metric</td>
<td>string</td>
<td>What is measured by the behavior.</td>
</tr>
<tr>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_:]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>criteria</td>
<td>BehaviorCriteria</td>
<td>The criteria that determine if a device is behaving normally in regard to the metric.</td>
</tr>
<tr>
<td>comparisonOperator</td>
<td>string</td>
<td>The operator that relates the thing measured (metric) to the criteria (value).</td>
</tr>
<tr>
<td>enum: less-than</td>
<td>less-than-equals</td>
<td>greater-than</td>
</tr>
<tr>
<td>value</td>
<td>MetricValue</td>
<td>The value to be compared with the metric.</td>
</tr>
<tr>
<td>count</td>
<td>long</td>
<td>If the comparisonOperator calls for a numeric value, use this to specify that numeric value to be compared with the metric.</td>
</tr>
<tr>
<td>range- min:0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### ListViolationEvents

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cidrs</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of CIDRs, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>member: Cidr</td>
<td></td>
</tr>
<tr>
<td>ports</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of ports, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>member: Port</td>
<td></td>
</tr>
<tr>
<td>durationSeconds</td>
<td>integer</td>
<td>Use this to specify the period of time over which the behavior is evaluated, for those criteria which have a time dimension (for example, NUM_MESSAGES_SENT).</td>
</tr>
<tr>
<td>metricValue</td>
<td>MetricValue</td>
<td>The value of the metric (the measurement).</td>
</tr>
<tr>
<td>count</td>
<td>long</td>
<td>If the comparisonOperator calls for a numeric value, use this to specify that numeric value to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>range- min:0</td>
<td></td>
</tr>
<tr>
<td>cidrs</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of CIDRs, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>member: Cidr</td>
<td></td>
</tr>
<tr>
<td>ports</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of ports, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>member: Port</td>
<td></td>
</tr>
<tr>
<td>violationEventType</td>
<td>string</td>
<td>The type of violation event.</td>
</tr>
<tr>
<td></td>
<td>enum: in-alarm</td>
<td>alarm-cleared</td>
</tr>
<tr>
<td>violationEventTime</td>
<td>timestamp</td>
<td>The time the violation event occurred.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

**Errors:**

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
ThrottlingException
- The rate exceeds the limit.

InternalFailureException
- An unexpected error has occurred.

UpdateSecurityProfile

Updates a Device Defender security profile.

https

Request syntax:

```
PATCH /security-profiles/securityProfileName?expectedVersion=expectedVersion
Content-type: application/json

{
    "securityProfileDescription": "string",
    "behaviors": [
        {
            "name": "string",
            "metric": "string",
            "criteria": {
                "comparisonOperator": "string",
                "value": {
                    "count": "long",
                    "cidrs": [
                        "string"
                    ],
                    "ports": [
                        "integer"
                    ]
                },
                "durationSeconds": "integer"
            }
        },
        "alertTargets": {
            "string": {
                "alertTargetArn": "string",
                "roleArn": "string"
            }
        }
    ]
}
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>yes</td>
<td>The name of the security profile you want to update.</td>
</tr>
<tr>
<td>expectedVersion</td>
<td>OptionalVersion</td>
<td>no</td>
<td>The expected version of the security profile. A new version is generated whenever the security profile is updated. If you</td>
</tr>
</tbody>
</table>
**UpdateSecurityProfile**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>specify a value that is different than the actual version, a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>VersionConflictException is thrown.</td>
</tr>
<tr>
<td>securityProfileDescription</td>
<td>SecurityProfileDescription</td>
<td>no</td>
<td>A description of the security profile.</td>
</tr>
<tr>
<td>behaviors</td>
<td>Behaviors</td>
<td>no</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>alert.</td>
</tr>
<tr>
<td>alertTargets</td>
<td>AlertTargets</td>
<td>no</td>
<td>Where the alerts are sent. (Alerts are always sent to the console.)</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileDescription</td>
<td>SecurityProfileDescription</td>
<td>no</td>
<td>A description of the security profile.</td>
</tr>
<tr>
<td>behaviors</td>
<td>Behaviors</td>
<td>no</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>alert.</td>
</tr>
<tr>
<td>alertTargets</td>
<td>AlertTargets</td>
<td>no</td>
<td>Where the alerts are sent. (Alerts are always sent to the console.)</td>
</tr>
</tbody>
</table>

**Response syntax:**

```json
{  
  "securityProfileName": "string",
  "securityProfileArn": "string",
  "securityProfileDescription": "string",
  "behaviors": [
    
    "name": "string",
    "metric": "string",
    "criteria": {
      "comparisonOperator": "string",
      "value": {
        "count": "long",
        "cids": [
          "string"
        ],
        "ports": [
          "integer"
        ],
        "durationSeconds": "integer"
      }
    },
  
  "alertTargets": {
    
    "string": {
      "alertTargetArn": "string",
      "roleArn": "string"
    }
  },
  
  "version": "long",
  "creationDate": "timestamp",
} ```
"lastModifiedDate": "timestamp"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>no</td>
<td>The name of the security profile that was updated.</td>
</tr>
<tr>
<td>securityProfileArn</td>
<td>SecurityProfileArn</td>
<td>no</td>
<td>The ARN of the security profile that was updated.</td>
</tr>
<tr>
<td>securityProfileDescription</td>
<td>SecurityProfileDescription</td>
<td>no</td>
<td>The description of the security profile.</td>
</tr>
<tr>
<td>behaviors</td>
<td>Behaviors</td>
<td>no</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td>alertTargets</td>
<td>AlertTargets</td>
<td>no</td>
<td>Where the alerts are sent. (Alerts are always sent to the console.)</td>
</tr>
<tr>
<td>version</td>
<td>Version</td>
<td>no</td>
<td>The updated version of the security profile.</td>
</tr>
<tr>
<td>creationDate</td>
<td>Timestamp</td>
<td>no</td>
<td>The time the security profile was created.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>Timestamp</td>
<td>no</td>
<td>The time the security profile was last modified.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

VersionConflictException

An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

HTTP response code: 409

ThrottlingException

The rate exceeds the limit.
HTTP response code: 429
InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

cli

Synopsis:

```
aws iot update-security-profile \
  --security-profile-name <value> \
  [--security-profile-description <value>] \
  [--behaviors <value>] \
  [--alert-targets <value>] \
  [--expected-version <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "securityProfileName": "string",
  "securityProfileDescription": "string",
  "behaviors": [
    {
      "name": "string",
      "metric": "string",
      "criteria": {
        "comparisonOperator": "string",
        "value": {
          "count": "long",
          "cidrs": ["string"],
          "ports": ["integer"]
        }
      },
      "durationSeconds": "integer"
    }
  ],
  "alertTargets": {
    "string": {
      "alertTargetArn": "string",
      "roleArn": "string"
    }
  },
  "expectedVersion": "long"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name of the security profile you want to update.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

511
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileDescription</td>
<td>string</td>
<td>A description of the security profile.</td>
</tr>
<tr>
<td>length- max:1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pattern: [\p{Graph}]*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>behaviors</td>
<td>list</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the behavior.</td>
</tr>
<tr>
<td>length- max:128 min:1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>metric</td>
<td>string</td>
<td>What is measured by the behavior.</td>
</tr>
<tr>
<td>criteria</td>
<td>BehaviorCriteria</td>
<td>The criteria that determine if a device is behaving normally in regard to the metric.</td>
</tr>
<tr>
<td>comparisonOperator</td>
<td>string</td>
<td>The operator that relates the thing measured (metric) to the criteria (value).</td>
</tr>
<tr>
<td>value</td>
<td>MetricValue</td>
<td>The value to be compared with the metric.</td>
</tr>
<tr>
<td>count</td>
<td>long</td>
<td>If the comparisonOperator calls for a numeric value, use this to specify that numeric value to be compared with the metric.</td>
</tr>
<tr>
<td>cidrs</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of CIDRs, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>ports</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of ports, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>durationSeconds</td>
<td>integer</td>
<td>Use this to specify the period of time over which the behavior is evaluated, for those criteria which have a time dimension (for example, NUM_MESSAGES_SENT).</td>
</tr>
<tr>
<td>alertTargets</td>
<td>map</td>
<td>Where the alerts are sent. (Alerts are always sent to the console.)</td>
</tr>
<tr>
<td>alertTargetArn</td>
<td>string</td>
<td>The ARN of the notification target to which alerts are sent.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants permission to send alerts to the notification target.</td>
</tr>
<tr>
<td>expectedVersion</td>
<td>long</td>
<td>The expected version of the security profile. A new version is generated whenever the security profile is updated. If you specify a value that is different than the actual version, a VersionConflictException is thrown.</td>
</tr>
</tbody>
</table>

Output:

```json
{
  "securityProfileName": "string",
  "securityProfileArn": "string",
  "securityProfileDescription": "string",
  "behaviors": [
    {
      "name": "string",
      "metric": "string",
      "criteria": {
        "comparisonOperator": "string",
        "value": {
          "count": "long",
          "cidrs": [
            "string"
          ],
          "ports": [
            "integer"
          ]
        },
        "durationSeconds": "integer"
      }
    }
  ],
  "alertTargets": {
    "string": {
      "alertTargetArn": "string",
      "roleArn": "string"
    }
  },
  "version": "long"
}
```
cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name of the security profile that was updated.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>securityProfileArn</td>
<td>string</td>
<td>The ARN of the security profile that was updated.</td>
</tr>
<tr>
<td>securityProfileDescription</td>
<td>string</td>
<td>The description of the security profile.</td>
</tr>
<tr>
<td></td>
<td>length- max:1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: \p{Graph}*</td>
<td></td>
</tr>
<tr>
<td>behaviors</td>
<td>list</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td></td>
<td>member: Behavior</td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the behavior.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>metric</td>
<td>string</td>
<td>What is measured by the behavior.</td>
</tr>
<tr>
<td>criteria</td>
<td>BehaviorCriteria</td>
<td>The criteria that determine if a device is behaving normally in regard to the metric.</td>
</tr>
<tr>
<td>comparisonOperator</td>
<td>string</td>
<td>The operator that relates the thing measured (metric) to the criteria (value).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: less-than</td>
</tr>
<tr>
<td>value</td>
<td>MetricValue</td>
<td>The value to be compared with the metric.</td>
</tr>
<tr>
<td>count</td>
<td>long</td>
<td>If the comparisonOperator calls for a numeric value, use this to specify that numeric value to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>range- min:0</td>
<td></td>
</tr>
<tr>
<td>cidrs</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of CIDRs, use</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>member: Cidr</td>
<td></td>
<td>this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>ports</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of ports, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>durationSeconds</td>
<td>integer</td>
<td>Use this to specify the period of time over which the behavior is evaluated, for those criteria which have a time dimension (for example, NUM_MESSAGES_SENT).</td>
</tr>
<tr>
<td>alertTargets</td>
<td>map</td>
<td>Where the alerts are sent. (Alerts are always sent to the console.)</td>
</tr>
<tr>
<td>alertTargetArn</td>
<td>string</td>
<td>The ARN of the notification target to which alerts are sent.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants permission to send alerts to the notification target.</td>
</tr>
<tr>
<td>version</td>
<td>long</td>
<td>The updated version of the security profile.</td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The time the security profile was created.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>timestamp</td>
<td>The time the security profile was last modified.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

**ResourceNotFoundException**

The specified resource does not exist.

**VersionConflictException**

An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

**ThrottlingException**

The rate exceeds the limit.

**InternalFailureException**

An unexpected error has occurred.
ValidateSecurityProfileBehaviors

Validates a Device Defender security profile behaviors specification.

Request syntax:

POST /security-profile-behaviors/validate
Content-type: application/json

{
  "behaviors": [
    {
      "name": "string",
      "metric": "string",
      "criteria": {
        "comparisonOperator": "string",
        "value": {
          "count": "long",
          "cidrs": [
            "string"
          ],
          "ports": [
            "integer"
          ],
          "durationSeconds": "integer"
        }
      }
    }
  ]
}

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>behaviors</td>
<td>Behaviors</td>
<td>yes</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{
  "valid": "boolean",
  "validationErrors": [
    {
      "errorMessage": "string"
    }
  ]
}
Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>valid</td>
<td>Valid</td>
<td>no</td>
<td>True if the behaviors were valid.</td>
</tr>
<tr>
<td>validationErrors</td>
<td>ValidationErrors</td>
<td>no</td>
<td>The list of any errors found in the behaviors.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot validate-security-profile-behaviors \
  --behaviors <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "behaviors": [
    {
      "name": "string",
      "metric": "string",
      "criteria": {
        "comparisonOperator": "string",
        "value": {
          "count": "long",
          "cidsrs": [
            "string"
          ],
          "ports": [
            "integer"
          ]
        },
        "durationSeconds": "integer"
      }
    }
  ]
}
```
### cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type/Pattern</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>behaviors</td>
<td>list member: Behavior</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td>name</td>
<td>string length- max:128 min:1 pattern: [a-zA-Z0-9:_-]+</td>
<td>The name you have given to the behavior.</td>
</tr>
<tr>
<td>metric</td>
<td>string</td>
<td>What is measured by the behavior.</td>
</tr>
<tr>
<td>criteria</td>
<td>BehaviorCriteria</td>
<td>The criteria that determine if a device is behaving normally in regard to the metric.</td>
</tr>
<tr>
<td>comparisonOperator</td>
<td>string</td>
<td>The operator that relates the thing measured (metric) to the criteria (value).</td>
</tr>
<tr>
<td>value</td>
<td>MetricValue</td>
<td>The value to be compared with the metric.</td>
</tr>
<tr>
<td>count</td>
<td>long range- min:0</td>
<td>If the comparisonOperator calls for a numeric value, use this to specify that numeric value to be compared with the metric.</td>
</tr>
<tr>
<td>cidrs</td>
<td>list member: Cidr</td>
<td>If the comparisonOperator calls for a set of CIDRs, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>ports</td>
<td>list member: Port</td>
<td>If the comparisonOperator calls for a set of ports, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>durationSeconds</td>
<td>integer</td>
<td>Use this to specify the period of time over which the behavior is evaluated, for those criteria which have a time dimension (for example, NUM_MESSAGES_SENT).</td>
</tr>
</tbody>
</table>
Device Agent Integration with AWS IoT Greengrass

AWS IoT Device Defender can be used in conjunction with AWS Greengrass. Device agent integration follows the standard Greengrass Lambda function deployment model, allowing you to add AWS IoT Device Defender security to your Greengrass Core devices. To integrate a device agent, follow the steps outlined in this section.

Prerequisites:

- Have your Greengrass environment set up.
- Have your Greengrass core configured and running.
- Ensure you can successfully deploy and run a Lambda function on your Greengrass core.

In general, the process described here follows the Create and Package a Lambda Function section of the AWS Greengrass Developers Guide.
Create A Lambda Package

1. Clone the AWS IoT Device Defender Python Samples Repository.
   ```
   git clone https://github.com/aws-samples/aws-iot-device-defender-agent-sdk-python.git
   ```
2. Create and activate a virtual environment (optional but recommended).
   ```
   pip install virtualenv
   virtualenv metrics_lambda_environment
   source metrics_lambda_environment/bin/activate
   ```
3. Install the AWS IoT Device Defender sample agent in the virtual environment Install from PyPi.
   ```
   pip install AWSIoTDeviceDefenderAgentSDK
   ```
4. Install the downloaded source.
   ```
   cd aws-iot-device-defender-agent-sdk-python
   #This must be run from the same directory as setup.py
   pip install .
   ```
5. Create an empty directory to assemble your Lambda function, we will refer to this as your “Lambda directory”.
   ```
   mkdir metrics_lambda
   cd metrics_lambda
   ```
6. Complete steps 1-4 from this section: Create and Package a Lambda Function.
7. Unzip the Greengrass python sdk into your Lambda directory.
   ```
   unzip ../aws_greengrass_core_sdk/sdk/python_sdk_1_1_0.zip
   cp -R ../aws_greengrass_core_sdk/examples/HelloWorld/greengrass_common .
   cp -R ../aws_greengrass_core_sdk/examples/HelloWorld/greengrasssdk .
   cp -R ../aws_greengrass_core_sdk/examples/HelloWorld/greengrass_ipc_python_sdk .
   ```
8. Copy the AWSIoTDeviceDefenderAgentSDK module to the root level of your Lambda directory.
   ```
   cp -R ../aws-iot-device-defender-agent-sdk-python/AWSIoTDeviceDefenderAgentSDK .
   ```
9. Copy the Greengrass agent to the root level of your Lambda directory.
   ```
   cp ../aws-iot-device-defender-agent-sdk-python/samples/greengrass/greengrass_core_metrics_agent/greengrass_defender_agent.py .
   ```
10. Customize the Greengrass agent to include the name of your Greengrass Core device, and the desired metrics sample rate:
    - Replace **GREENGRASS_CORENAME** with the name of your Greengrass Core.
    - Set the **SAMPLE_RATE_SECONDS** to your desired metrics reporting interval. (Note: 5 minutes (300 seconds) is the shortest reporting interval supported by AWS IoT Device Defender.)
11. Copy the dependencies from your virtual environment (or your system) into the the root level of your Lambda directory.
    ```
    cp -R ../metrics_lambda_environment/lib/python2.7/site-packages/psutil .
    cp -R ../metrics_lambda_environment/lib/python2.7/site-packages/cbor .
    ```
12. Create your Lambda function zipfile. (Note: you should perform this command in the root level of your Lambda directory.)

```
rm *.zip
zip -r greengrass_defender_metrics_lambda.zip *
```

**Configure and deploy your Greengrass Lambda function**

1. **Upload your lambda zip file.**
2. Select the Python 2.7 runtime, and enter `greengrass_defender_agent.function_handler` in the Handler field.
3. **Configure your lambda as a long-lived lambda.**
4. **Configure a subscription from your Lambda function to the AWS IoT Cloud.** (Note: For AWS IoT Device Defender, a subscription from the AWS IoT cloud to your Lambda function is not required.)
5. Create a local resource to allow your Lambda function to collect metrics from your Greengrass Core host:
   - Follow the instructions [here](#) using the following parameters:
     - Resource Name: Core Proc
     - Type: Volume
     - Source Path: /proc
     - Destination Path: /host_proc
     - Group owner file access permission: “Automatically add OS group permissions of the Linux group that owns the resource”
     - Associate the resource with your metrics Lambda function.
6. Deploy your Lambda function to your Greengrass Group.

**Review your Device Defender device metrics using the AWS IoT Console**

1. Temporarily modify the publish topic in your Greengrass Lambda function to "metrics/test".
2. Deploy the Lambda function.
3. Add a subscription to the temporary topic ("metrics/test") in the "Test" section of the IoT console in order to see the metrics your Greengrass Core is emitting.

---

**Security Best Practices for Device Agents**

**Least Privilege**

The agent process should granted only the minimum permissions necessary to perform its duties.

**Basic Mechanisms**

- Agent should be run as non-root user.
- Agent should run as a dedicated user, in it's own group.
- User/groups should be granted Read-Only permissions on the resources required to gather and transmit metrics.
- Example: read-only on /proc /sys for the sample agent.
- For an example of how to setup a process to run with reduced permissions, see the Setup Instructions which are included with the Python Sample Agent.
There are a number of well-known Linux mechanisms that can help you further restrict/isolate your agent process:

**Advanced Mechanisms**

- CGroups
- SELinux
- Chroot
- Linux Namespaces

**Operational Resiliency**

An agent process must be resilient to unexpected operational errors and exceptions and must not crash or exit permanently. The code needs to gracefully handle exceptions and, as a precaution, it must be configured to automatically restart in case of unexpected termination (for example, due to system restarts or uncaught exceptions).

**Least Dependencies**

An agent must use the least possible number of dependencies (i.e. third-party libraries) in its implementation. If use of a library is justified due to the complexity of a task (for example, transport layer security) only use well-maintained dependencies and establish a mechanism to keep dependencies up to date. If the added dependencies contain functionality not used by the agent and active by default (for example, opening ports, domain sockets), disable them in your code or by means of the library's configuration files.

**Process Isolation**

An agent process must only contain functionality required for performing device metric gathering and transmission. It must not piggyback on other system processes as a container or implement functionality for other out of scope use-cases. Additionally, the agent process must refrain from creating inbound communication channels such as domain socket and network service ports which would allow local or remote processes to interfere with its operation and impact its integrity and isolation.

**Stealthiness**

An agent process must not be named with keywords such as security, monitoring, or audit indicating its purpose and security value. Generic code names or random and unique-per-device process names must be preferred. The same principle must be followed in naming the directory in which the agent's binaries reside and any names and values of process arguments.

**Least Information Shared**

Any agent artifacts deployed to devices must not contain sensitive information such as privileged credentials, debugging and dead code, or inline comments or documentation files which reveal details about server-side processing of agent-gathered metrics or other details about backend systems.

**Transport Layer Security**

To establish TLS secure channels for data transmission, an agent process must enforce all client-side validations, such as certificate chain and domain name validation, at the application level, if not enabled by default. Furthermore, an agent must use a root certificate store which contains trusted authorities and does not contain certificates belonging to compromised certificate issuers.

**Secure Deployment**

Any agent deployment mechanism, such as code push or sync and repositories containing its binaries, source code and any configuration files (including trusted root certificates), must be access controlled to prevent unauthorized code injection or tampering. If the deployment mechanism relies on network communication, then cryptographic methods must be utilized to protect the integrity of deployment artifacts in transit.
Device Defender Troubleshooting Guide

General

Q: Are there any prerequisites to using Device Defender?

A: You can use the Device Defender Detect feature for devices that are registered as things with AWS IoT. To use the cloud-side metrics, devices must connect using the thing name as their client Id.

Audit

Q: I enabled a check and my audit has been showing "In-Progress“ for a long time. Is something wrong? When will I get results?

A: When a check is enabled, data collection begins immediately. However, if you have a large amount of data in your account to be collected (certificates, things, policies, etc.) then the results of the check may not be available for some time after you have enabled it.

Detect

Q: How do I know what thresholds should be set in an AWS IoT Device Defender security profile behavior?

A: Start by creating a security profile behavior with low thresholds and attach it to a thing group consisting of a representative set of devices. Device defender will alert you with the metric datapoints emitted by the device for the behaviors that are violated. You can then fine-tune the device behavior thresholds to match your use case.

Q: I created a behavior, but it is not triggering a violation when I expect it to. How should I fix it?

A: Keep in mind that when you define a behavior you are indicating how you expect your device to behave normally. For example, if you have a security camera that only connects to one central server on TCP port 8888, you don’t expect it to make any other connections. To be alerted if the camera makes a connection on another port, you could define a behavior such as:

```json
{
    "name": "Listening TCP Ports",
    "metric": "aws:listening-tcp-ports",
    "criteria": {
        "comparisonOperator": "in-port-set",
        "value": {
            "ports": [ 8888 ]
        }
    }
}
```
Once the behavior has been created, if the camera makes a TCP connection on TCP Port 443, the device behavior would be violated and would trigger an alert.

Q: One or more of my behaviors are in violation. How do I clear the violation?

A: Alarms will clear once the device returns to expected behavior, as defined by the behavior profiles you have defined. Behavior profiles are evaluated upon receipt of metrics data for your device.

Q: I deleted a behavior that was in violation, how do I stop the alerts?

A: Deleting a behavior will stop all future violations and alerts for that behavior. Prior alerts will need to be drained from your notification mechanism as normal. However, when a behavior is deleted, the record of violations of that behavior will be retained for the same time period as all other violations in your account.

**Device Metrics**

Q: I’m submitting metrics reports that I know violate my behaviors, but no violations are being triggered. What’s wrong?

A: Check that your metrics reports are being accepted by subscribing to the following MQTT topics:

```plaintext
$aws/things/THING_NAME/defender/metrics/FORMAT/rejected
$aws/things/THING_NAME/defender/metrics/FORMAT/accepted
```

where “THING_NAME” is the name of the thing reporting the metric and FORMAT is either “json” or “cbor” depending on the format of the metrics report the thing submits.

After you have subscribed, you should receive messages on these topics for each metric report submitted. A "rejected" message indicates that there was a problem parsing the metric report. An error message is included in the message payload to help you correct any errors in your metric report. An "accepted" message indicates the metric report was parsed properly.

Q: What happens if I send an empty metric in my metric report?

A: An empty list of ports or IP addresses is always considered in conformity with the corresponding behavior. If the corresponding behavior was in violation, then the violation will be cleared.

Q: My device metric reports are getting rejected with an error message of "XXXX Not a Thing". How can I fix it?

A: Make sure you are submitting metrics for a thing which is registered in your AWS IoT account. Device Defender requires things to be registered in your account to evaluate reported metrics against defined behaviors.

If you are submitting metrics from a registered thing, verify that you are sending a well-formed metrics report using one of the supported formats. ([Device Metrics Document Specification (p. 468)](https://docs.aws.amazon.com/iot/latest/developerguide/device-metrics.html))

Q: What value should I supply in the report id field in my device metrics report?

A: This should be a unique value for each metric report, expressed as a positive integer. A common practice is to use a Unix epoch timestamp.

Q: Should I create a dedicated MQTT connection for Device Defender metrics?

A: A separate MQTT connection is not required.

Q: What client id should I use when connecting to publish device metrics?

You should use a registered thing name as the clientId when connecting to AWS IoT.
Q: Can I publish metrics for a device with a different clientId?

It is possible to publish metrics on behalf of another thing, as long as that thing is registered in your AWS account. This can be accomplished by publishing the metrics to the Device Defender reserved topic for that device. For example, "Thing-1" would like to publish metrics for itself and also on behalf of "Thing-2". "Thing-1" collects its own metrics and publishes them on the MQTT topic:

```
/aws/things/Thing-1/defender/metrics/json
```

"Thing-1" will then obtain metrics from "Thing-2" and publish these metrics on the MQTT topic:

```
/aws/things/Thing-2/defender/metrics/json
```

As long as "Thing-1" and "Thing-2" are registered in your account, metric submission and evaluation will work properly.

Q: How many security profiles and behaviors can I have in my account?

A: Refer to the Detect Service Limits (p. 467) section of the AWS IoT Device Defender Developer Guide.

Q: What does a prototypical target role for an alert target look like?

A: A role that allows AWS IoT Device Defender to publish alerts on an alert target (SNS topic) requires 2 things:
1. a trust relationship specifying iot.amazonaws.com as the trusted entity and
2. an attached policy which grants AWS IoT permission to publish on a specified SNS topic, for example:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sns:Publish",
            "Resource": "<sns-topic-arn>"
        }
    ]
}
```
AWS IoT Events

AWS IoT publishes event messages when certain events occur. For example, events are generated by the Registry when things are added, updated, or deleted. Each event causes a single event message to be sent. Event messages are published over MQTT with a JSON payload. The content of the payload depends on the type of event.

You control which event types are published by calling the UpdateEventConfigurations API.

You can get the current event configuration by calling the DescribeEventConfigurations API.

In order to receive event messages your device must use an appropriate policy that allows it to connect to the AWS IoT device gateway and subscribe to MQTT event topics. You must also subscribe to the appropriate topic filters.

The following is an example of the policy required for receiving lifecycle events:

```json
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "iot:Subscribe",
                "iot:Receive"
            ],
            "Resource":[
                "arn:aws:iot:region:account:/aws/events/*"
            ]
        }
    ]
}
```

Note
Event messages are guaranteed to be published once. It is possible for them to be published more than once. The ordering of event messages is not guaranteed.

Registry Events

The Registry publishes event messages when things, thing types, and thing groups are created, updated, or deleted. The Registry currently supports the following event types:

**Thing Created/Updated/Deleted**

The Registry publishes the following event messages when things are created, updated, or deleted:

- `$aws/events/thing/<thingName>/created`
- `$aws/events/thing/<thingName>/updated`
- `$aws/events/thing/<thingName>/deleted`

The messages contain the following example payload:

```json
{
    "eventType" : "thingEvent",
    "eventId" : "f5ae9b94-8b8e-4d8e-8c8f-b3266dd89853",
}
```
"timestamp" : 1234567890123,
"operation" : "CREATED|UPDATED|DELETED",
"accountld" : "123456789012",
"thingId" : "b604f69c-aa9a-4d4a-829e-c480e958a0b5",
"thingName" : "MyThing",
"versionNumber" : 1,
"thingTypeName" : null,
"attributes": {
    "attribute3": "value3",
    "attribute1": "value1",
    "attribute2": "value2"
}
}

The payloads contain the following attributes:

**eventType**

Set to "thingEvent".

**eventId**

A unique event ID (string).

**timestamp**

The UNIX timestamp of when the event occurred.

**operation**

The operation that triggered the event. Valid values are:

- CREATED
- UPDATED
- DELETED

**accountId**

Your AWS account ID.

**thingId**

The ID of the thing being created, updated, or deleted.

**thingName**

The name of the thing being created, updated, or deleted.

**versionNumber**

The version of the thing being created, updated, or deleted. This value is set to 1 when a thing is created. It is incremented by 1 each time the thing is updated.

**thingTypeName**

The thing type associated with the thing, if one exists. Otherwise, null.

**attributes**

A collection of name-value pairs associated with the thing.

### Thing Type Created/Deprecated/Undeprecated/Deleted

The Registry publishes the following event messages when thing types are created, deprecated, undeprecated, or deleted:

- $aws/events/thingType/<thingTypeName>/created
- $aws/events/thing/<thingTypeName>/updated
- $aws/events/thing/<thingTypeName>/deleted
The message contains the following example payload:

```
{
  "eventType" : "thingTypeEvent",
  "eventId" : "8827376c-4b05-49a3-9b3b-733729df7ed5",
  "timestamp" : 1234567890123,
  "operation" : "CREATED|UPDATED|DELETED",
  "accountId" : "123456789012",
  "thingTypeId" : "c530ae83-32aa-4592-94d3-da29879daaac",
  "thingTypeName" : "MyThingType",
  "isDeprecated" : false|true,
  "deprecationDate" : null,
  "searchableAttributes" : [ "attribute1", "attribute2", "attribute3" ],
  "description" : "My thing type"
}
```

The payloads contain the following attributes:

- **eventType**
  - Set to "thingTypeEvent".

- **eventId**
  - A unique event ID (string).

- **timestamp**
  - The UNIX timestamp of when the event occurred.

- **operation**
  - The operation that triggered the event. Valid values are:
    - CREATED
    - UPDATED
    - DELETED

- **accountId**
  - Your AWS account ID.

- **thingTypeId**
  - The ID of the thing type being created, deprecated, or deleted.

- **thingTypeName**
  - The name of the thing type being created, deprecated, or deleted.

- **isDeprecated**
  - true if the thing type is deprecated. Otherwise, false.

- **deprecationDate**
  - The UNIX timestamp for when the thing type was deprecated.

- **searchableAttributes**
  - A collection of name-value pairs associated with the thing type that can be used for searching.

- **description**
  - A description of the thing type.

**Thing Type Associated/Disassociated With a Thing**

The Registry publishes the following event messages when a thing type is associated or disassociated with a thing.
The messages contain the following example payload:

```json
{
    "eventId" : "87f8e095-531c-47b3-aab5-5171364d138d",
    "eventType" : "THING_TYPE_ASSOCIATION_EVENT",
    "operation" : "CREATED|DELETED",
    "thingId" : "b604f69c-aa9a-4d4a-829e-c480e958a0b5",
    "thingName" : "myThing",
    "thingTypeName" : "MyThingType",
    "timestamp" : 1234567890123,
}
```

The payloads contain the following attributes:

- **eventId**
  A unique event ID (string).

- **eventType**
  Set to "THING_TYPE_ASSOCIATION_EVENT".

- **operation**
  The operation that triggered the event. Valid values are:
  - CREATED
  - DELETED

- **thingId**
  The ID of the thing whose type association was changed.

- **thingName**
  The name of the thing whose type association was changed.

- **thingTypeName**
  The thing type associated with, or no longer associated with, the thing.

- **timestamp**
  The UNIX timestamp of when the event occurred.

### Thing Group Created/Updated/Deleted

The Registry publishes the following event messages when a thing group is created, updated or deleted.

- `$aws/events/thingGroup/<groupName>/created`
- `$aws/events/thingGroup/<groupName>/updated`
- `$aws/events/thingGroup/<groupName>/deleted`

The messages contain the following example payload:

```json
{
    "eventType" : "thingGroupEvent",
    "eventId" : "87f8e095-531c-47b3-aab5-5171364d138d",
    "timestamp" : 1234567890123,
    "operation" : "CREATED|UPDATED|DELETED",
    "accountId" : "123456789012",
    "thingGroupId" : "8f82a106-6b1d-4331-8984-a84db5f6f8cb",
    "thingGroupName" : "MyRootThingGroup",
}
```
"versionNumber" : 1,
"parentGroupName" : null,
"parentGroupId" : null,
"description" : "My root thing group",
"rootToParentThingGroups" : null,
"attributes" : {
   "attribute1" : "value1",
   "attribute3" : "value3",
   "attribute2" : "value2"
}
}

The payloads contain the following attributes:

**eventType**
- Set to "thingGroupEvent".

**eventId**
- A unique event ID (string).

**timestamp**
- The UNIX timestamp of when the event occurred.

**operation**
- The operation that triggered the event. Valid values are:
  - CREATED
  - UPDATED
  - DELETED

**accountId**
- Your AWS account ID.

**thingGroupId**
- The ID of the thing group being created, updated, or deleted.

**thingGroupName**
- The name of the thing group being created, updated, or deleted.

**versionNumber**
- The version of the thing group. This value is set to 1 when a thing group is created. It is incremented by 1 each time the thing group is updated.

**parentGroupName**
- The name of the parent thing group (if one exists).

**parentGroupId**
- The ID of the parent thing group (if one exists).

**description**
- A description of the thing group.

**rootToParentThingGroups**
- An array of information about the parent thing group. There is one entry for each parent thing group, starting with the parent of the current thing group and continuing until the root thing group has been reached. Each entry contains the thing group name and the thing group ARN.
attributes

A collection of name-value pairs associated with the thing group.

Thing Added To/Removed From a Thing Group

The Registry publishes the following event messages when a thing is added to or removed from a thing group:

- `$aws/events/thingGroupMembership/thingGroup/<thingGroupName>/thing/<thingName>/added`
- `$aws/events/thingGroupMembership/thingGroup/<thingGroupName>/thing/<thingName>/removed`

The messages contain the following example payload:

```json
{
    "eventType" : "thingGroupMembershipEvent",
    "eventId" : "d684bd5f-6f6e-48e1-950c-766ac7f02fd1",
    "timestamp" : 1234567890123,
    "operation" : "ADDED|REMOVED",
    "accountId" : "123456789012",
    "groupId" : "06838589-373f-4312-b1f2-53f2192291c4",
    "thingId" : "b604f69c-aa9a-4d4a-829e-c480e958a0b5",
    "membershipId" : "8505ebf8-4d32-4286-80e9-c23a4a16bbd8"
}
```

The payloads contain the following attributes:

- **eventType**
  - Set to "thingGroupMembershipEvent".
- **eventId**
  - The event ID.
- **timestamp**
  - The UNIX timestamp for when the event occurred.
- **operation**
  - **ADDED** when a thing is added to a thing group. **REMOVED** when a thing is removed from a thing group.
- **accountId**
  - Your AWS account ID.
- **groupArn**
  - The ARN of the thing group.
- **groupId**
  - The ID of the group.
- **thingArn**
  - The ARN of the thing that was added or removed from the thing group.
- **thingId**
  - The ID of the thing that was added or removed from the thing group.
membershipId

An ID that represents the relationship between the thing and the thing group. This value is generated when you add a thing to a thing group.

Thing Group Added To/Deleted From Thing Group

The Registry publishes the following event messages when a thing group is added to or removed from another thing group.

• $aws/events/thingGroupHierarchy/thingGroup/<parentThingGroupName>/childThingGroup/<childThingGroupName>/added

• $aws/events/thingGroupHierarchy/thingGroup/<parentThingGroupName>/childThingGroup/<childThingGroupName>/removed

The message contains the following example payload:

```
{
    "eventType" : "thingGroupHierarchyEvent",
    "eventId" : "264192c7-b573-46ef-ab7b-489fcd47da41",
    "timestamp" : 1234567890123,
    "operation" : "ADDED|REMOVED",
    "accountId" : "123456789012",
    "thingGroupId" : "8f82a106-6b1d-4331-8984-a84db5f6f8cb",
    "thingGroupName" : "MyRootThingGroup",
    "childGroupId" : "06838589-373f-4312-b1f2-53f2192291c4",
    "childGroupName" : "MyChildThingGroup"
}
```

The payloads contain the following attributes:

**eventType**

Set to "thingGroupHierarchyEvent".

**eventId**

The event ID.

**timestamp**

The UNIX timestamp for when the event occurred.

**operation**

ADDED when a thing is added to a thing group. REMOVED when a thing is removed from a thing group.

**accountId**

Your AWS account ID.

**thingGroupId**

The ID of the parent thing group.

**thingGroupName**

The name of the parent thing group.

**childGroupId**

The ID of the child thing group.

**childGroupName**

The name of the child thing group.
Jobs publishes to reserved topics on the MQTT protocol when jobs are pending, completed, or canceled, and when a device reports success or failure when executing a job. Devices or management and monitoring applications can keep track of the status of jobs by subscribing to these topics. You need to use the UpdateEventConfigurations API to control what kinds of job events you receive. See IoT Events for more information.

Job Completed/Canceled

AWS IoT Jobs publishes a message on an MQTT topic when a job is completed or canceled:

- $aws/events/job/jobID/completed
- $aws/events/job/jobID/canceled

The "completed" message contains the following example payload:

```json
{
   "eventType": "JOB",
   "eventId": "7364ffd1-8b65-4824-85d5-6c14686c97c6",
   "timestamp": 1234567890,
   "operation": "completed",
   "jobId": "27450507-bf6f-4012-92af-bb8a1c8c4484",
   "status": "COMPLETED",
   "targetSelection": "SNAPSHOT|CONTINUOUS",
   "targets": [
      "arn:aws:iot:us-east-1:123456789012:thing/a39f6f91-70cf-4bd2-a381-9c66df1a80d0",
      "arn:aws:iot:us-east-1:123456789012:thinggroup/2fc4c0a4-6e45-4e45-4525-a238-0fe8d3dd21bb"
   ],
   "description": "My Job Description",
   "createdAt": 1234567890123,
   "lastUpdatedAt": 1234567890123,
   "jobProcessDetails": {
      "numberOfCanceledThings": 0,
      "numberOfRejectedThings": 0,
      "numberOfFailedThings": 0,
      "numberOfRemovedThings": 0,
      "numberOfSucceededThings": 3
   }
}
```

The "canceled" message contains the following example payload:

```json
{
   "eventType": "JOB",
   "eventId": "568d2ade-2e9c-46e6-a115-18afa1286b06",
   "timestamp": 1234567890,
   "operation": "canceled",
   "jobId": "4d2a531a-da2e-47bb-8b9e-ff5adcd53ef0",
   "status": "CANCELED",
   "targetSelection": "SNAPSHOT|CONTINUOUS",
   "targets": [
      "arn:aws:iot:us-east-1:123456789012:thing/Thing0-947b9c0c-ff10-4a80-b4b3-cd33d0145a0f",
      "arn:aws:iot:us-east-1:123456789012:thinggroup/ThingGroup1-95c644d5-1621-41a6-9aa5-ad2de581d18f"
   ],
   "description": "My job description",
   "createdAt": 1234567890123,
   "lastUpdatedAt": 1234567890123
}
```
Job Execution Terminal Status

AWS IoT Jobs publishes a message when a device updates a job execution to terminal status:

- `$aws/events/jobExecution/jobID/succeeded`
- `$aws/events/jobExecution/jobID/failed`
- `$aws/events/jobExecution/jobID/rejected`
- `$aws/events/jobExecution/jobID/canceled`
- `$aws/events/jobExecution/jobID/removed`

The message contains the following example payload:

```json
{
    "eventType": "JOB_EXECUTION",
    "eventId": "cca89fa5-8a7f-4ced-8c20-5e653af3572",
    "timestamp": 1234567890,
    "operation": "succeeded|failed|rejected|canceled|removed",
    "jobId": "154b39e5-60b0-48a4-9b73-f6f80d032d27",
    "thingArn": "arn:aws:iot:us-east-1:123456789012:myThing/6d639fbc-8f85-4a90-924d-a2867f8366a7",
    "status": "SUCCEEDED|FAILED|REJECTED|CANCELED|REMOVED",
    "statusDetails": {
        "key": "value"
    }
}
```
AWS IoT SDKs

Contents
- AWS Mobile SDK for Android (p. 535)
- Arduino Yún SDK (p. 535)
- AWS IoT Device SDK for Embedded C (p. 535)
- AWS IoT C++ Device SDK (p. 536)
- AWS Mobile SDK for iOS (p. 536)
- AWS IoT Device SDK for Java (p. 536)
- AWS IoT Device SDK for JavaScript (p. 536)
- AWS IoT Device SDK for Python (p. 537)

The AWS IoT Device SDKs help you to easily and quickly connect your devices to AWS IoT. The AWS IoT Device SDKs include open-source libraries, developer guides with samples, and porting guides so that you can build innovative IoT products or solutions on your choice of hardware platforms.

AWS Mobile SDK for Android

The AWS SDK for Android contains a library, samples, and documentation for developers to build connected mobile applications using AWS. This SDK also includes support for calling AWS IoT APIs. For more information, see the following:
- AWS Mobile SDK for Android on GitHub
- AWS Mobile SDK for Android Readme
- AWS Mobile SDK for Android Samples

Arduino Yún SDK

The AWS IoT Arduino Yún SDK makes it possible for developers to connect their Arduino Yún-compatible boards to AWS IoT. By connecting a device to AWS IoT, users can securely work with the message broker, rules, and shadows provided by AWS IoT and with other AWS services like AWS Lambda, Kinesis, and Amazon S3. For more information, see the following:
- Arduino Yún SDK on GitHub
- Arduino Yún SDK Readme

AWS IoT Device SDK for Embedded C

The AWS IoT Device SDK for Embedded C is a collection of C source files that can be used in embedded applications to securely connect to the AWS IoT platform. It includes transport clients, TLS implementations, and examples for their use. It also supports AWS IoT-specific features such as an API to access the Device Shadow service. It is distributed as source code and is intended to be built into
customer firmware along with application code, other libraries, and RTOS. For more information, see the following:

- AWS IoT Device SDK for Embedded C GitHub
- AWS IoT Device SDK for Embedded C Readme
- AWS IoT Device SDK for Embedded C Porting Guide

AWS IoT C++ Device SDK

The AWS IoT C++ Device SDK allows developers to build connected applications using AWS and the AWS IoT APIs. Specifically, this SDK was designed for devices that are not resource constrained and required advanced features such as message queuing, multi-threading support, and the latest language features. For more information, see the following:

- AWS IoT C++ Device SDK GitHub
- AWS IoT C++ Device SDK Readme

AWS Mobile SDK for iOS

The AWS SDK for iOS is an open-source software development kit, distributed under an Apache Open Source license. The SDK for iOS provides a library, code samples, and documentation to help developers build connected mobile applications using AWS. This SDK also includes support for calling the AWS IoT API.

- AWS SDK for iOS on GitHub
- AWS SDK for iOS Readme
- AWS SDK for iOS Samples

AWS IoT Device SDK for Java

The AWS IoT Device SDK for Java makes it possible for Java developers to access the AWS IoT platform through MQTT or MQTT over the WebSocket protocol. The SDK is built with shadow support. You can access shadows by using HTTP methods, including GET, UPDATE, and DELETE. The SDK also supports a simplified shadow access model, which allows developers to exchange data with shadows by just using getter and setter methods, without having to serialize or deserialize any JSON documents. For more information, see the following:

- AWS IoT Device SDK for Java on GitHub
- AWS IoT Device SDK for Java readme

AWS IoT Device SDK for JavaScript

The aws-iot-device-sdk.js package makes it possible for developers to write JavaScript applications that access AWS IoT using MQTT or MQTT over the WebSocket protocol. It can be used in Node.js environments and browser applications. For more information, see the following:

- AWS IoT Device SDK for JavaScript on GitHub
- AWS IoT Device SDK for JavaScript readme
AWS IoT Device SDK for Python

The AWS IoT Device SDK for Python makes it possible for developers to write Python scripts to use their devices to access the AWS IoT platform through MQTT or MQTT over the WebSocket protocol. By connecting their devices to AWS IoT, users can securely work with the message broker, rules, and shadows provided by AWS IoT and with other AWS services like AWS Lambda, Kinesis, and Amazon S3, and more.

- AWS IoT Device SDK for Python on GitHub
- AWS IoT Device SDK for Python readme
Monitoring AWS IoT

Monitoring is an important part of maintaining the reliability, availability, and performance of AWS IoT and your AWS solutions. You should collect monitoring data from all parts of your AWS solution so that you can more easily debug a multi-point failure if one occurs. Before you start monitoring AWS IoT, you should create a monitoring plan that includes answers to the following questions:

- What are your monitoring goals?
- Which resources will you monitor?
- How often will you monitor these resources?
- Which monitoring tools will you use?
- Who will perform the monitoring tasks?
- Who should be notified when something goes wrong?

The next step is to establish a baseline for normal AWS IoT performance in your environment, by measuring performance at various times and under different load conditions. As you monitor AWS IoT, store historical monitoring data so that you can compare it with current performance data, identify normal performance patterns and performance anomalies, and devise methods to address issues.

For example, if you're using Amazon EC2, you can monitor CPU utilization, disk I/O, and network utilization for your instances. When performance falls outside your established baseline, you might need to reconfigure or optimize the instance to reduce CPU utilization, improve disk I/O, or reduce network traffic.

To establish a baseline you should, at a minimum, monitor the following items:

- PublishIn.Success
- PublishOut.Success
- Subscribe.Success
- Ping.Success
- Connect.Success
- GetThingShadow.Accepted
- UpdateThingShadow.Accepted
- DeleteThingShadow.Accepted
- RulesExecuted

Topics

- Monitoring Tools (p. 538)
- Monitoring with Amazon CloudWatch (p. 539)
- Logging AWS IoT API Calls with AWS CloudTrail (p. 549)

Monitoring Tools

AWS provides various tools that you can use to monitor AWS IoT. You can configure some of these tools to do the monitoring for you, while some of the tools require manual intervention. We recommend that you automate monitoring tasks as much as possible.
Automated Monitoring Tools

You can use the following automated monitoring tools to watch AWS IoT and report when something is wrong:

- **Amazon CloudWatch Alarms** – Watch a single metric over a time period that you specify, and perform one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The action is a notification sent to an Amazon Simple Notification Service (Amazon SNS) topic or Amazon EC2 Auto Scaling policy. CloudWatch alarms do not invoke actions simply because they are in a particular state; the state must have changed and been maintained for a specified number of periods. For more information, see Monitoring with Amazon CloudWatch (p. 539).

- **Amazon CloudWatch Logs** – Monitor, store, and access your log files from AWS CloudTrail or other sources. For more information, see Monitoring Log Files in the Amazon CloudWatch User Guide.

- **Amazon CloudWatch Events** – Match events and route them to one or more target functions or streams to make changes, capture state information, and take corrective action. For more information, see What is Amazon CloudWatch Events in the Amazon CloudWatch User Guide.

- **AWS CloudTrail Log Monitoring** – Share log files between accounts, monitor CloudTrail log files in real time by sending them to CloudWatch Logs, write log processing applications in Java, and validate that your log files have not changed after delivery by CloudTrail. For more information, see Working with CloudTrail Log Files in the AWS CloudTrail User Guide.

Manual Monitoring Tools

Another important part of monitoring AWS IoT involves manually monitoring those items that the CloudWatch alarms don’t cover. The AWS IoT, CloudWatch, and other AWS console dashboards provide an at-a-glance view of the state of your AWS environment. We recommend that you also check the log files on AWS IoT.

- **AWS IoT dashboard** shows:
  - CA certificates
  - Certificates
  - Polices
  - Rules
  - Things

- **CloudWatch home page** shows:
  - Current alarms and status
  - Graphs of alarms and resources
  - Service health status

In addition, you can use CloudWatch to do the following:

- Create customized dashboards to monitor the services you care about
- Graph metric data to troubleshoot issues and discover trends
- Search and browse all your AWS resource metrics
- Create and edit alarms to be notified of problems

Monitoring with Amazon CloudWatch

You can monitor AWS IoT using CloudWatch, which collects and processes raw data from AWS IoT into readable, near real-time metrics. These statistics are recorded for a period of two weeks, so that you can access historical information and gain a better perspective on how your web application or service is...
AWS IoT Developer Guide
Metrics and Dimensions

performing. By default, AWS IoT metric data is automatically sent to CloudWatch in 1 minute periods.
For more information, see What Are Amazon CloudWatch, Amazon CloudWatch Events, and Amazon
CloudWatch Logs? in the Amazon CloudWatch User Guide.

Topics
• AWS IoT Metrics and Dimensions (p. 540)
• How Do I Use AWS IoT Metrics? (p. 547)
• Creating CloudWatch Alarms to Monitor AWS IoT (p. 547)

AWS IoT Metrics and Dimensions

When you interact with AWS IoT, it sends the following metrics and dimensions to CloudWatch every
minute. You can use the following procedures to view the metrics for AWS IoT.

To view metrics using the CloudWatch console

Metrics are grouped first by the service namespace, and then by the various dimension combinations
within each namespace.
2. In the navigation pane, choose Metrics.
3. In the CloudWatch Metrics by Category pane, under the metrics category for AWS IoT, select a
metrics category, and then in the upper pane, scroll down to view the full list of metrics.

To view metrics using the AWS CLI

• At a command prompt, use the following command:

```
aws cloudwatch list-metrics --namespace "AWS/IoT"
```

CloudWatch displays the following metrics for AWS IoT:

AWS IoT Metrics

The AWS/IoT namespace includes the following metrics. AWS IoT sends the following metrics to
CloudWatch once per received request.

**IoT Metrics**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RulesExecuted</td>
<td>The number of AWS IoT rules executed.</td>
</tr>
</tbody>
</table>

**Rule Metrics**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TopicMatch</td>
<td>The number of incoming messages published on a topic on which a rule is listening. The RuleName dimension contains the name of the rule.</td>
</tr>
<tr>
<td>ParseError</td>
<td>The number of JSON parse errors that occurred in messages published on a topic on which a rule is</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>listening. The RuleName dimension contains the name of the rule.</td>
</tr>
</tbody>
</table>

**Rule Action Metrics**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The number of successful rule action invocations. The RuleName dimension contains the name of the rule that specifies the action. The ActionType dimension contains the type of action that was invoked.</td>
</tr>
<tr>
<td>Failure</td>
<td>The number of failed rule action invocations. The RuleName dimension contains the name of the rule that specifies the action. The RuleName dimension contains the name of the rule that specifies the action. The ActionType dimension contains the type of action that was invoked.</td>
</tr>
</tbody>
</table>

**Message Broker Metrics**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect.AuthError</td>
<td>The number of connection requests that could not be authorized by the message broker. The Protocol dimension contains the protocol used to send the CONNECT message.</td>
</tr>
<tr>
<td>Connect.ClientError</td>
<td>The number of connection requests rejected because the MQTT message did not meet the requirements defined in AWS IoT Limits. The Protocol dimension contains the protocol used to send the CONNECT message.</td>
</tr>
<tr>
<td>Connect.ServerError</td>
<td>The number of connection requests that failed because an internal error occurred. The Protocol dimension contains the protocol used to send the CONNECT message.</td>
</tr>
<tr>
<td>Connect.Success</td>
<td>The number of successful connections to the message broker. The Protocol dimension contains the protocol used to send the CONNECT message.</td>
</tr>
<tr>
<td>Connect.Throttle</td>
<td>The number of connection requests that were throttled because the client exceeded the allowed connect request rate. The Protocol dimension contains the protocol used to send the CONNECT message.</td>
</tr>
<tr>
<td>Ping.Success</td>
<td>The number of ping messages received by the message broker. The Protocol dimension contains the protocol used to send the ping message.</td>
</tr>
<tr>
<td>PublishIn.AuthError</td>
<td>The number of publish requests the message broker was unable to authorize. The Protocol dimension contains the protocol used to publish the message.</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PublishIn.ClientError</td>
<td>The number of publish requests rejected by the message broker because the message did not meet the requirements defined in AWS IoT Limits. The Protocol dimension contains the protocol used to publish the message.</td>
</tr>
<tr>
<td>PublishIn.ServerError</td>
<td>The number of publish requests the message broker failed to process because an internal error occurred. The Protocol dimension contains the protocol used to send the PUBLISH message.</td>
</tr>
<tr>
<td>PublishIn.Success</td>
<td>The number of publish requests successfully processed by the message broker. The Protocol dimension contains the protocol used to send the PUBLISH message.</td>
</tr>
<tr>
<td>PublishIn.Throttle</td>
<td>The number of publish request that were throttled because the client exceeded the allowed inbound message rate. The Protocol dimension contains the protocol used to send the PUBLISH message.</td>
</tr>
<tr>
<td>PublishOut.AuthError</td>
<td>The number of publish requests made by the message broker that could not be authorized by AWS IoT. The Protocol dimension contains the protocol used to send the PUBLISH message.</td>
</tr>
<tr>
<td>PublishOut.ClientError</td>
<td>The number of publish requests made by the message broker that were rejected because the message did not meet the requirements defined in AWS IoT Limits. The Protocol dimension contains the protocol used to send the PUBLISH message.</td>
</tr>
<tr>
<td>PublishOut.Success</td>
<td>The number of publish requests successfully made by the message broker. The Protocol dimension contains the protocol used to send the PUBLISH message.</td>
</tr>
<tr>
<td>Subscribe.AuthError</td>
<td>The number of subscription requests made by a client that could not be authorized. The Protocol dimension contains the protocol used to send the SUBSCRIBE message.</td>
</tr>
<tr>
<td>Subscribe.ClientError</td>
<td>The number of subscribe requests that were rejected because the SUBSCRIBE message did not meet the requirements defined in AWS IoT Limits. The Protocol dimension contains the protocol used to send the SUBSCRIBE message.</td>
</tr>
<tr>
<td>Subscribe.ServerError</td>
<td>The number of subscribe requests that were rejected because an internal error occurred. The Protocol dimension contains the protocol used to send the SUBSCRIBE message.</td>
</tr>
<tr>
<td>Subscribe.Success</td>
<td>The number of subscribe requests that were successfully processed by the message broker. The Protocol dimension contains the protocol used to send the SUBSCRIBE message.</td>
</tr>
</tbody>
</table>
## Metrics and Dimensions

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscribe.Throttle</td>
<td>The number of subscribe requests that were throttled because the client exceeded the allowed subscribe request rate. The Protocol dimension contains the protocol used to send the SUBSCRIBE message.</td>
</tr>
<tr>
<td>Unsubscribe.ClientError</td>
<td>The number of unsubscribe requests that were rejected because the UNSUBSCRIBE message did not meet the requirements defined in AWS IoT Limits. The Protocol dimension contains the protocol used to send the UNSUBSCRIBE message.</td>
</tr>
<tr>
<td>Unsubscribe.ServerError</td>
<td>The number of unsubscribe requests that were rejected because an internal error occurred. The Protocol dimension contains the protocol used to send the UNSUBSCRIBE message.</td>
</tr>
<tr>
<td>Unsubscribe.Success</td>
<td>The number of unsubscribe requests that were successfully processed by the message broker. The Protocol dimension contains the protocol used to send the UNSUBSCRIBE message.</td>
</tr>
<tr>
<td>Unsubscribe.Throttle</td>
<td>The number of unsubscribe requests that were rejected because the client exceeded the allowed unsubscribe request rate. The Protocol dimension contains the protocol used to send the UNSUBSCRIBE message.</td>
</tr>
</tbody>
</table>

**Note**
The message broker metrics are displayed in the AWS IoT console under Protocol Metrics.

### Device Shadow Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeleteThingShadow.Accepted</td>
<td>The number of DeleteThingShadow requests processed successfully. The Protocol dimension contains the protocol used to make the request.</td>
</tr>
<tr>
<td>GetThingShadow.Accepted</td>
<td>The number of GetThingShadow requests processed successfully. The Protocol dimension contains the protocol used to make the request.</td>
</tr>
<tr>
<td>UpdateThingShadow.Accepted</td>
<td>The number of UpdateThingShadow requests processed successfully. The Protocol dimension contains the protocol used to make the request.</td>
</tr>
</tbody>
</table>

**Note**
The device shadow metrics are displayed in the AWS IoT console under Protocol Metrics.

### Jobs Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerError</td>
<td>The number of server errors generated while executing the job. The JobId dimension contains the ID of the job.</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ClientError</td>
<td>The number of client errors generated while executing the job. The JobId dimension contains the ID of the job.</td>
</tr>
<tr>
<td>QueuedJobExecutionTotalCount</td>
<td>The total number of job executions whose status is QUEUED for the given job. The JobId dimension contains the ID of the job.</td>
</tr>
<tr>
<td>InProgressJobExecutionTotalCount</td>
<td>The total number of job executions whose status is IN_PROGRESS for the given job. The JobId dimension contains the ID of the job.</td>
</tr>
<tr>
<td>FailedJobExecutionTotalCount</td>
<td>The total number of job executions whose status is FAILED for the given job. The JobId dimension contains the ID of the job.</td>
</tr>
<tr>
<td>SucceededJobExecutionTotalCount</td>
<td>The total number of job executions whose status is SUCCESS for the given job. The JobId dimension contains the ID of the job.</td>
</tr>
<tr>
<td>CanceledJobExecutionTotalCount</td>
<td>The total number of job executions whose status is CANCELED for the given job. The JobId dimension contains the ID of the job.</td>
</tr>
<tr>
<td>RejectedJobExecutionTotalCount</td>
<td>The total number of job executions whose status is REJECTED for the given job. The JobId dimension contains the ID of the job.</td>
</tr>
<tr>
<td>RemovedJobExecutionTotalCount</td>
<td>The total number of job executions whose status is REMOVED for the given job. The JobId dimension contains the ID of the job.</td>
</tr>
<tr>
<td>QueuedJobExecutionCount</td>
<td>The number of job executions whose status has changed to QUEUED within a time period that is determined by CloudWatch. (For more information about CloudWatch metrics, see Amazon CloudWatch Metrics.) The JobId dimension contains the ID of the job.</td>
</tr>
<tr>
<td>InProgressJobExecutionCount</td>
<td>The number of job executions whose status has changed to IN_PROGRESS within a time period that is determined by CloudWatch. (For more information about CloudWatch metrics, see Amazon CloudWatch Metrics.) The JobId dimension contains the ID of the job.</td>
</tr>
<tr>
<td>FailedJobExecutionCount</td>
<td>The number of job executions whose status has changed to FAILED within a time period that is determined by CloudWatch. (For more information about CloudWatch metrics, see Amazon CloudWatch Metrics.) The JobId dimension contains the ID of the job.</td>
</tr>
</tbody>
</table>
### AWS IoT Developer Guide

**Metrics and Dimensions**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SucceededJobExecutionCount</strong></td>
<td>The number of job executions whose status has changed to SUCCESS within a time period that is determined by CloudWatch. (For more information about CloudWatch metrics, see Amazon CloudWatch Metrics.) The JobId dimension contains the ID of the job.</td>
</tr>
<tr>
<td><strong>CanceledJobExecutionCount</strong></td>
<td>The number of job executions whose status has changed to CANCELED within a time period that is determined by CloudWatch. (For more information about CloudWatch metrics, see Amazon CloudWatch Metrics.) The JobId dimension contains the ID of the job.</td>
</tr>
<tr>
<td><strong>RejectedJobExecutionCount</strong></td>
<td>The number of job executions whose status has changed to REJECTED within a time period that is determined by CloudWatch. (For more information about CloudWatch metrics, see Amazon CloudWatch Metrics.) The JobId dimension contains the ID of the job.</td>
</tr>
<tr>
<td><strong>RemovedJobExecutionCount</strong></td>
<td>The number of job executions whose status has changed to REMOVED within a time period that is determined by CloudWatch. (For more information about CloudWatch metrics, see Amazon CloudWatch Metrics.) The JobId dimension contains the ID of the job.</td>
</tr>
</tbody>
</table>

**Device Defender Audit Metrics**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NonCompliantResources</strong></td>
<td>The number of resources that were found to be non-compliant with a check. The system will report the number of resources which were out of compliance for each check of each audit performed.</td>
</tr>
<tr>
<td><strong>ResourcesEvaluated</strong></td>
<td>The number of resources that were evaluated for compliance. The system will report the number of resources which were evaluated for each check of each audit performed.</td>
</tr>
</tbody>
</table>

**Device Defender Detect Metrics**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Violations</strong></td>
<td>The number of new violations of security profile behaviors that have been found since the last time an evaluation was performed. The system will report the number of new violations for the account, for a specific security profile, and for a specific behavior of a specific security profile.</td>
</tr>
<tr>
<td><strong>ViolationsCleared</strong></td>
<td>The number of violations of security profile behaviors that have resolved since the last time an evaluation was performed.</td>
</tr>
</tbody>
</table>
was performed. The system will report the number of resolved violations for the account, for a specific security profile, and for a specific behavior of a specific security profile.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ViolationsInvalidated</td>
<td>The number of violations of security profile behaviors for which information is no longer available since the last time an evaluation was performed (because the reporting device stopped reporting, or is no longer being monitored for some reason). The system will report the number of invalidated violations for the entire account, for a specific security profile, and for a specific behavior of a specific security profile.</td>
</tr>
</tbody>
</table>

**Dimensions for Metrics**

Metrics use the namespace and provide metrics for the following dimension(s):

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActionType</td>
<td>The action type specified by the rule that triggered by the request.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol used to make the request. Valid values are: MQTT or HTTP.</td>
</tr>
<tr>
<td>RuleName</td>
<td>The name of the rule triggered by the request.</td>
</tr>
<tr>
<td>JobId</td>
<td>The ID of the job whose progress or message connection success/failure is being monitored.</td>
</tr>
<tr>
<td>TaskType</td>
<td>The type of Device Defender Audit whose check results are being monitored. One of &quot;SCHEDULED_AUDIT_TASK&quot; or &quot;ON_DEMAND_AUDIT_TASK&quot;.</td>
</tr>
<tr>
<td>CheckName</td>
<td>The name of the Device Defender audit check whose results are being monitored.</td>
</tr>
<tr>
<td>ScheduledAuditName</td>
<td>The name of the Device Defender scheduled audit whose check results are being monitored. This will have the value &quot;OnDemand&quot; if the results reported are for an audit that was performed on-demand.</td>
</tr>
<tr>
<td>SecurityProfileName</td>
<td>The name of the Device Defender Detect security profile whose behaviors are being monitored.</td>
</tr>
<tr>
<td>BehaviorName</td>
<td>The name of the Device Defender Detect security profile behavior which is being monitored.</td>
</tr>
</tbody>
</table>
How Do I Use AWS IoT Metrics?

The metrics reported by AWS IoT provide information that you can analyze in different ways. The following use cases are based on a scenario where you have ten things that connect to the internet once a day. Each day:

- Ten things connect to AWS IoT at roughly the same time.
- Each thing subscribes to a topic filter, and then waits for an hour before disconnecting. During this period, things communicate with one another and learn more about the state of the world.
- Each thing publishes some perception it has based on its newly found data using UpdateThingShadow.
- Each thing disconnects from AWS IoT.

These are suggestions to get you started, not a comprehensive list.

- How can I be notified if my things do not connect successfully each day? (p. 547)
- How can I be notified if my things are not publishing data each day? (p. 548)
- How can I be notified if my thing's shadow updates are being rejected each day? (p. 548)

Creating CloudWatch Alarms to Monitor AWS IoT

You can create a CloudWatch alarm that sends an Amazon SNS message when the alarm changes state. An alarm watches a single metric over a time period you specify and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The action is a notification sent to an Amazon SNS topic or Auto Scaling policy. Alarms invoke actions for sustained state changes only. CloudWatch alarms do not invoke actions simply because they are in a particular state; the state must have changed and been maintained for a specified number of periods.

How can I be notified if my things do not connect successfully each day?


2. Create the alarm.

```
Prompt>aws cloudwatch put-metric-alarm \
   --alarm-name ConnectSuccessAlarm \ 
   --alarm-description "Alarm when my Things don't connect successfully" \ 
   --namespace AWS/IoT \ 
   --metric-name Connect.Success \ 
   --dimensions Name=Protocol,Value=MQTT \ 
   --statistic Sum \ 
   --threshold 10 \ 
   --comparison-operator LessThanThreshold \ 
   --period 86400 \ 
   --unit Count \ 
   --evaluation-periods 1 \ 
```

3. Test the alarm.
How can I be notified if my things are not publishing data each day?

   For more information, see Set Up Amazon Simple Notification Service.

2. Create the alarm.

```bash
Prompt>aws cloudwatch put-metric-alarm
   --alarm-name PublishInSuccessAlarm
   --alarm-description "Alarm when my Things don't publish their data"
   --namespace AWS/IoT
   --metric-name PublishIn.Success
   --dimensions Name=Protocol,Value=MQTT
   --statistic Sum
   --threshold 10
   --comparison-operator LessThanThreshold
   --period 86400
   --unit Count
   --evaluation-periods 1
```

3. Test the alarm.

```bash
Prompt>aws cloudwatch set-alarm-state --alarm-name PublishInSuccessAlarm --state-reason "initializing" --state-value OK

Prompt>aws cloudwatch set-alarm-state --alarm-name PublishInSuccessAlarm --state-reason "initializing" --state-value ALARM
```

How can I be notified if my thing's shadow updates are being rejected each day?

   For more information, see Set Up Amazon Simple Notification Service.

2. Create the alarm.

```bash
Prompt>aws cloudwatch put-metric-alarm
   --alarm-name UpdateThingShadowSuccessAlarm
   --alarm-description "Alarm when my Things Shadow updates are getting rejected"
   --namespace AWS/IoT
   --metric-name UpdateThingShadow.Success
   --dimensions Name=Protocol,Value=MQTT
   --statistic Sum
```

548
Log the AWS IoT API Calls with AWS CloudTrail

AWS IoT is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS IoT. CloudTrail captures all API calls for AWS IoT as events, including calls from the AWS IoT console and from code calls to the AWS IoT APIs. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for AWS IoT. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the information collected by CloudTrail, you can determine the request that was made to AWS IoT, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

AWS IoT Information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in AWS IoT, that activity is recorded in a CloudTrail event along with other AWS service events in Event history. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for AWS IoT, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all regions. The trail logs events from all regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see:

- Overview for Creating a Trail
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

Note

AWS IoT data plane actions (device side) are not logged by CloudTrail. Use CloudWatch to monitor these.

AWS IoT control plane actions are logged by CloudTrail. For example, calls to the CreateThing, ListThings, and ListTopicRules sections generate entries in the CloudTrail log files.
Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or IAM user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity Element. AWS IoT actions are documented in the AWS IoT API Reference.

### Understanding AWS IoT Log File Entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files are not an ordered stack trace of the public API calls, so they do not appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the AttachPolicy action.

```json
{
    "timestamp":"1460159496",
    "AdditionalEventData":"
    "Annotation":"
    "ApiVersion":"
    "ErrorCode":"
    "ErrorMessage":"
    "EventID":"8bff4fed-c229-4d2d-8264-4ab28a487505",
    "EventName":"AttachPolicy",
    "EventTime":"2016-04-08T23:51:36Z",
    "EventTypeDef":"AwsApiCall",
    "ReadOnly":"
    "RecipientAccountList":"
    "RequestID":"d4875df2-fde4-11e5-b829-23bf9b56c6cd",
    "RequestParameters":{
        "principal":"
        "policyName":"
    },
    "Resources":"
    "ResponseElements":"
    "SourceIpAddress":"52.90.213.26",
    "UserAgent":"
    "UserIdentity":{
        "type":"AssumedRole",
        "principalId":"
        "arn":"
        "account":"
        "accessKeyId":"
        "mfaAuthenticated":false
        "creationDate":Fri Apr 08 23:51:10 UTC 2016"
    },
    "sessionIssuer":{
        "type":"
        "principalId":"
        "arn":"
    }
}
```
"accountId": "222222222222",
"userName": "iotmonitor-us-east-1-InstanceRole-1C5T1YC3YHFYT"
}
},
"invokedBy":{
  "serviceAccountId": "111111111111"
}
},
"VpcEndpointId": ""
Troubleshooting AWS IoT

The following information might help you troubleshoot common issues in AWS IoT.

Tasks
- Diagnosing Connectivity Issues (p. 552)
- Setting Up CloudWatch Logs with AWS IoT (p. 552)
- Diagnosing Problems with Shadows (p. 571)
- Diagnosing Salesforce IoT Input Stream Action Issues (p. 572)
- AWS IoT Limits (p. 573)
- AWS IoT Errors (p. 573)

Diagnosing Connectivity Issues

Authentication

How do my devices authenticate AWS IoT endpoints?

Add the AWS IoT CA certificate to your client’s trust store. You can download the CA certificate from here.

How can I validate a correctly configured certificate?

Use the OpenSSL s_client command to test a connection to the AWS IoT endpoint:

```bash
openssl s_client -connect custom_endpoint.iot.us-east-1.amazonaws.com:8443 -CAfile CA.pem -cert cert.pem -key privateKey.pem
```

Authorization

I received a PUBNACK or SUBNACK response from the broker. What do I do?

Make sure that there is a policy attached to the certificate you are using to call AWS IoT. All publish/subscribe operations are denied by default.

Setting Up CloudWatch Logs with AWS IoT

AWS IoT sends progress events about each message as it passes from your devices through the message broker and the rules engine. To view these logs, you must configure AWS IoT to generate the logs used by CloudWatch.

For more information about CloudWatch Logs in general, see CloudWatch Logs. For information on supported AWS IoT CloudWatch Logs, see CloudWatch Log Entry Format (p. 556) below.

To enable AWS IoT logging, you must create an IAM role, register the role with AWS IoT, and then configure AWS IoT logging.
Create a Logging Role

Use the IAM console to create a logging role.

1. From the navigation pane, choose Roles, and then choose Create new role.
2. Choose AWS Service Role and for service role type, choose AWS IoT.
3. Choose the AWSIoTLogging role, and then choose Next Step.
4. Type a name and description for the role, and then choose Create role.

Logging Role Policy

The following policy documents provide the role policy and trust policy that allow AWS IoT to submit logs to CloudWatch on your behalf.

Note
These documents were created for you when you created the logging role.

Role policy:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "logs:CreateLogGroup",
            "logs:CreateLogStream",
            "logs:PutLogEvents",
            "logs:PutMetricFilter",
            "logs:PutRetentionPolicy"
         ],
         "Resource": [
            "*"
         ]
      }
   ]
}
```

Trust policy:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "",
         "Effect": "Allow",
         "Principal": {
            "Service": "iot.amazonaws.com"
         },
         "Action": "sts:AssumeRole"
      }
   ]
}
```
Log Level

The log level specifies which types of logs are generated.

ERROR

Any error that causes an operation to fail.

Logs include ERROR information only.

WARN

Anything that can potentially cause inconsistencies in the system, but might not cause the operation to fail.

Logs include ERROR and WARN information.

INFO

High-level information about the flow of things.

Logs include INFO, ERROR, and WARN information.

DEBUG

Information that might be helpful when debugging a problem.

Logs include DEBUG, INFO, ERROR, and WARN information.

DISABLED

All logging is disabled.

Configure AWS IoT Logging

You can configure logging in two ways, global logging and fine grained logging. Global logging sets one logging level for all logs no matter what resource triggered the logs. Fine-grained logging allows you to set a logging level for a specific resource or set of resources. Currently only thing groups are supported.

Global Logging

Use the `set-v2-logging-options` CLI command to set the logging options for your account. `set-v2-logging-options` takes three arguments:

--role-arn

Your logging role ARN. The logging role grants AWS IoT permission to write to your CloudWatch Logs.

--default-log-level

The log level to use. Valid values are: ERROR, WARN, INFO, DEBUG, or DISABLED

--disable-all-logs | --no-disable-all-logs

When set to true (--disable-all-logs) disables all logs. The default (parameter not used) is false.
Configure AWS IoT Logging

For example:

```
aws iot set-v2-logging-options \\
  --role-arn arn:aws:iam::<your-aws-account-num>:role/<IoTLoggingRole> \\
  --default-log-level <INFO>
```

You can use the `get-v2-logging-options` CLI command to get the current logging options.

**Note**
AWS IoT continues to support older commands to set and get global logging on your account: `set-logging-options` and `get-logging-options`. Be aware that when these commands are used, the resulting logs will contain plain-text, rather than JSON payloads and logging latency will generally be higher. Also, no further improvements will be made to the implementation of these older commands. We recommend using the "v2" versions to configure your logging options and, when possible, changing any legacy applications which use the older versions.

**Fine-Grained Logging**

Fine-grained logging allows you to specify a logging level for a target. A target is defined by a resource type and a resource name. Currently, AWS IoT supports thing groups as targets. Fine-grained logging allows you to set a logging level for a specific thing group. Say we have a thing group called "Phones" that contains things that represent different kinds of phones. We then create another thing group called "MobilePhones" and make it a child of the "Phones" thing group. Fine-grained logging allows you to configure one logging level for all things in the "Phones" group (and any child groups) and another logging level for things in the "MobilePhones" group. In this example, we have assigned two different logging levels to things in the "MobilePhones" group — one from the logging level for the "Phones" thing group and another from the "MobilePhones" thing group — but the logging level specified for the child thing group will override the logging level specified for the parent thing group.

Use the `set-v2-logging-options` CLI command to enable fine-grained logging and set the default logging level. It takes the following optional arguments:

```
--role-arn

An IAM role that allows AWS IoT to write to your CloudWatch Logs. If not specified, AWS IoT uses the logging role associated with your account. The logging role is associated with your account when it is created. For more information, see Create a Logging Role (p. 553)

--default-log-level

The logging level used if not specified. Valid values are: DEBUG, INFO, ERROR, WARN, and DISABLED

--disable-all-logs | --no-disable-all-logs

When set to true (--disable-all-logs) disables all logs. The default (parameter not used) is false.
```

The `get-v2-logging-options` CLI command returns the configured IAM logging role, the default logging level, and the `disableAllLogs` value.

Use the `set-v2-logging-level` CLI command to configure fine-grained logging for a target. It takes the following arguments:

```
--log-target

A JSON object that contains the resource type (field `targetType`) and name (field `targetName`) of the entity for which you are configuring logging. AWS IoT currently supports `THING_GROUP` for the resource type. You can configure up to 10 logging targets.
--log-level

The logging level used when generating logs for the specified resource. Valid values are: DEBUG, INFO, ERROR, WARN, and DISABLED.

Use the list-v2-logging-levels CLI command to get a list of the currently configured fine-grained logging levels. Call the delete-v2-logging-level CLI command to delete a logging level. Use the delete-v2-logging-level command to delete a fine-grained logging level.

CloudWatch Log Entry Format

Each component of AWS IoT generates its own logs. Each log entry has an eventType that indicates which operation caused the log to be generated. This section describes the logs generated by the following AWS IoT components:

- Message Broker (p. 556)
- Device Shadow service (p. 560)
- Rules Engine (p. 562)
- Jobs (p. 566)

All CloudWatch Logs have the following common attributes:

timestamp

The UNIX timestamp of when the client connected to the AWS IoT message broker.

logLevel

The log level being used. For more information, see the section called “Log Level” (p. 554).

traceId

A randomly generated identifier that can be used to correlate all logs for a specific request.

accountId

Your AWS account ID.

status

The status of the request.

eventType

The event type for which the log was generated. The value of the event type for each event is listed in the following sections.

Message Broker Logs

The AWS IoT message broker generates logs for the following events:

Connect Log

The AWS IoT message broker generates a Connect log when an MQTT client connects.

more info (1)

For example:

```json
{
}
In addition to the attributes common to all CloudWatch Logs, Connect log entries contain the following attributes:

**eventType**
- Connect for connection logs.

**protocol**
- The protocol used when making the request. Valid values are MQTT or HTTP.

**clientId**
- The ID of the client making the request.

**principalId**
- The ID of the principal making the request.

**sourceIp**
- The IP address where the request originated.

**sourcePort**
- The port where the request originated.

### Subscribe Log

The AWS IoT message broker generates a Subscribe log when an MQTT client subscribes to a topic.

For example:

```json
{
  "timestamp": "2017-08-10 15:39:04.413",
  "logLevel": "INFO",
  "traceId": "7aa5c38d-1b49-3753-15dc-513ce4ab9fa6",
  "accountId": "123456789012",
  "status": "Success",
  "eventType": "Subscribe",
  "protocol": "MQTT",
  "topicName": "$aws/things/MyThing/shadow/#",
  "clientId": "abf2709286e49a8a5c1922749736453",
  "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafcc5a932167",
  "sourceIp": "205.251.233.181",
  "sourcePort": 13490
}
```

In addition to the attributes common to all CloudWatch Logs, Subscribe log entries contain the following attributes:
eventType

Subscribe for subscription logs.

protocol

The protocol used when making the request. Valid values are MQTT or HTTP.

topicName

The name of the subscribed topic.

clientId

The ID of the client making the request.

principalId

The ID of the principal making the request.

sourceIp

The IP address where the request originated.

sourcePort

The port where the request originated.

Publish-In Log

The AWS IoT message broker generates a Publish-In log when the AWS IoT message broker receives an MQTT message.

more info (3)

For example:

```
{
  "timestamp": "2017-08-10 15:39:30.961",
  "logLevel": "INFO",
  "traceId": "672ec480-31ce-fd8b-b5fb-22e3ac420699",
  "accountId": "123456789012",
  "status": "Success",
  "eventType": "Publish-In",
  "protocol": "MQTT",
  "topicName": "$aws/things/MyThing/shadow/get",
  "clientId": "abf2709286e49a8a5c1922749736453",
  "principalId": "145179c40e2219e1a909d896a5340b74cf97a39641beec2fc3eeafc5a932167",
  "sourceIp": "205.251.233.181",
  "sourcePort": 13490
}
```

In addition to the attributes common to all CloudWatch Logs, Publish-In log entries contain the following attributes:

eventType

Publish-In when the message broker receives a message.

status

The status of the request.

protocol

The protocol used when making the request. Valid values are MQTT or HTTP.
CloudWatch Log Entry Format

**topicName**

The name of the subscribed topic.

**clientId**

The ID of the client making the request.

**principalId**

The ID of the principal making the request.

**sourceIp**

The IP address where the request originated.

**sourcePort**

The port where the request originated.

### Publish-Out Log

The AWS IoT message broker generates a Publish-Out log when the message broker publishes an MQTT message.

For example:

```
{
    "timestamp": "2017-08-10 15:39:30.961",
    "logLevel": "INFO",
    "traceId": "672ec480-31ce-fd8b-b5fb-22e3ac420699",
    "accountId": "123456789012",
    "status": "Success",
    "eventType": "Publish-Out",
    "protocol": "MQTT",
    "topicName": "$aws/things/MyThing/shadow/get",
    "clientId": "abf270288649a8a5c1922749736453",
    "principalId": "145179c60e2219e18a909b896a5340b74cf97a39641beec2f3ec5a932167",
    "sourceIp": "205.251.233.181",
    "sourcePort": 13490
}
```

In addition to the attributes common to all CloudWatch Logs, Publish-Out log entries contain the following attributes:

**eventType**

Publish-Out when the message broker publishes a message.

**status**

The status of the request.

**protocol**

The protocol used when making the request. Valid values are MQTT or HTTP.

**topicName**

The name of the subscribed topic.

**clientId**

The ID of the client making the request.
principalId

The ID of the principal making the request.
sourceIp

The IP address where the request originated.
sourcePort

The port where the request originated.

Disconnect Log

The AWS IoT message broker generates a Disconnect log when an MQTT client disconnects.

For example:

```json
{
  "timestamp": "2017-08-10 15:37:23.476",
  "logLevel": "INFO",
  "traceId": "20b23f3f-d7f1-fee8-169f-f2263394fbdb",
  "accountId": "123456789012",
  "status": "Success",
  "eventType": "Disconnect",
  "protocol": "MQTT",
  "clientId": "abf27092886e49a8a5c1922749736453",
  "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeaf5a931267",
  "sourceIp": "205.251.233.181",
  "sourcePort": 13490
}
```

In addition to the attributes common to all CloudWatch Logs, Disconnect log entries contain the following attributes:

eventType

Disconnect for connection logs.

protocol

The protocol used when making the request. Valid values are MQTT or HTTP.

clientId

The ID of the client making the request.

principalId

The ID of the principal making the request.

sourceIp

The IP address where the request originated.

sourcePort

The port where the request originated.

Device Shadow Logs

The AWS IoT Device Shadow service generates logs for the following events:
GetThingShadow Logs

The Device Shadow service generates a GetThingShadow log when a get request for a shadow is received.

more info (6)

For example:

```
{
  "timestamp": "2017-08-09 17:56:30.941",
  "logLevel": "INFO",
  "traceId": "b575f19a-97a2-cf72-0ed0-c64a783a2504",
  "accountId": "123456789012",
  "status": "Success",
  "eventType": "GetThingShadow",
  "protocol": "MQTT",
  "deviceShadowName": "MyThing",
  "topicName": "$aws/things/MyThing/shadow/get"
}
```

In addition to the attributes common to all CloudWatch Logs, GetThingShadow log entries contain the following attributes:

**eventType**

GetThingShadow for GetThingShadow logs.

**protocol**

The protocol used when making the request. Valid values are MQTT or HTTP.

**deviceShadowName**

The name of the requested shadow.

**topicName**

The name of the topic on which the request was published.

UpdateThingShadow Logs

The Device Shadow service generates a UpdateThingShadow log when a request to update a device's shadow is received.

more info (7)

For example:

```
{
  "timestamp": "2017-08-07 18:43:59.436",
  "logLevel": "INFO",
  "traceId": "d0074ba8-0c4b-a400-69df-76326d414c28",
  "accountId": "123456789012",
  "status": "Success",
  "eventType": "UpdateThingShadow",
  "protocol": "MQTT",
  "deviceShadowName": "Jack",
  "topicName": "$aws/things/Jack/shadow/update"
}
```

In addition to the attributes common to all CloudWatch Logs, UpdateThingShadow log entries contain the following attributes:
eventType

UpdateThingShadow for update shadow logs.

protocol

The protocol used when making the request. Valid values are MQTT or HTTP.

deviceShadowName

The name of the shadow to update.

topicName

The name of the topic on which the request was published.

DeleteThingShadow Logs

The Device Shadow service generates a DeleteThingShadow log when a request to delete a device's shadow is received.

more info (8)

For example:

```
{
  "timestamp": "2017-08-07 18:47:56.664",
  "logLevel": "INFO",
  "traceId": "1a60d02e-15b9-605b-7096-a9f584a6ad3f",
  "accountId": "123456789012",
  "status": "Success",
  "eventType": "DeleteThingShadow",
  "protocol": "MQTT",
  "deviceShadowName": "Jack",
  "topicName": "$aws/things/Jack/shadow/delete"
}
```

In addition to the attributes common to all CloudWatch Logs, DeleteThingShadow log entries contain the following attributes:

eventType

DeleteThingShadow for DeleteThingShadow logs.

protocol

The protocol used when making the request. Valid values are MQTT or HTTP.

deviceShadowName

The name of the shadow to update.

topicName

The name of the topic on which the request was published.

Rules Engine Logs

The AWS IoT Rules Engine service generates logs for the following events:

Rule Match Logs

The AWS IoT rules engine generates a RuleMatch log when the message broker receives a message that matches a rule.
more info (9)

For example:

```
{
  "timestamp": "2017-08-10 16:32:46.002",
  "logLevel": "INFO",
  "traceId": "30aa7ccc-1d23-0b97-aa7b-76196d83537e",
  "accountId": "123456789012",
  "status": "Success",
  "eventType": "RuleMatch",
  "clientId": "abf27092886e49a8a5c1922749736453",
  "topicName": "rules/test",
  "ruleName": "JSONLogsRule",
  "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eaf5a932167"
}
```

In addition to the attributes common to all CloudWatch Logs, RuleMatch log entries contain the following attributes:

- **eventType**
  - `RuleMatch` for rule match logs.

- **clientId**
  - The ID of the client making the request.

- **topicName**
  - The name of the subscribed topic.

- **ruleName**
  - The name of the matching rule.

- **principalId**
  - The ID of the principal making the request.

Function Execution Logs

The rules engine generates a FunctionExecution log when a rule's SQL query calls an external function. An external function is called when a rule's action makes an HTTP request to AWS IoT or another web service (for example, calling `get_thing_shadow` or `machinelearning_predict`).

more info (10)

A FunctionExecution log will look like the following:

```
{
  "timestamp": "2017-07-13 18:33:51.903",
  "logLevel": "DEBUG",
  "traceId": "180532b7-0cc7-057b-687a-5ca1824830f5",
  "status": "Success",
  "eventType": "FunctionExecution",
  "clientId": "N/A",
  "topicName": "rules/test",
  "ruleName": "ruleTestPredict",
  "ruleAction": "MachinelearningPredict",
  "resources": {
    "ModelId": "predict-model"
  }
}
```
In addition to the attributes common to all CloudWatch Logs, FunctionExecution log entries contain the following attributes:

**eventType**

FunctionExecution for rule match logs.

**principalId**

N/A for FunctionExecution logs.

**topicName**

The name of the subscribed topic.

**ruleName**

The name of the matching rule.

**resources**

A collection of resources used by the rule's actions.

**principalId**

The ID of the principal making the request.

### Starting Execution Logs

The AWS IoT rules engine generates a StartingExecution log when the rules engine starts to invoke a rule's action.

For example:

```json
{
    "timestamp": "2017-08-10 16:32:46.002",
    "logLevel": "DEBUG",
    "traceId": "30aa7ccc-1d23-0b97-aa7b-76196d83537e",
    "accountId": "123456789012",
    "status": "Success",
    "eventType": "StartingRuleExecution",
    "clientId": "abf2709286e49a8a5c1922749736453",
    "topicName": "rules/test",
    "ruleName": "JSONLogsRule",
    "ruleAction": "RepublishAction",
    "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafc5a932167"
}
```

In addition to the attributes common to all CloudWatch Logs, StartingExecution log entries contain the following attributes:

**eventType**

StartingRuleExecution for starting rule execution logs.

**principalId**

The ID of the client making the request.
Rule Execution Logs

The AWS IoT rules engine generates a `RuleExecution` log when the rules engine invokes a rule's action.

For example:

```json
{
    "timestamp": "2017-08-10 16:32:46.070",
    "logLevel": "INFO",
    "traceId": "30aa7ccc-1d23-0b97-aa7b-76196d83537e",
    "accountId": "123456789012",
    "status": "Success",
    "eventType": "RuleExecution",
    "clientId": "abf27092886e49a8a5c1922749736453",
    "topicName": "rules/test",
    "ruleName": "JSONLogsRule",
    "ruleAction": "RepublishAction",
    "resources": {
        "RepublishTopic": "rules/republish"
    },
    "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eaf0c5a932167"
}
```

In addition to the attributes common to all CloudWatch Logs, `RuleExecution` log entries contain the following attributes:

- **eventType**
  - `RuleExecution` for rule execution logs.
- **clientId**
  - The ID of the client making the request.
- **topicName**
  - The name of the subscribed topic.
- **ruleName**
  - The name of the matching rule.
- **ruleAction**
  - The name of the invoked action.
- **resources**
  - A collection of resources used by the rule's actions.
principalId
The ID of the principal making the request.

Job Logs
The AWS IoT Job service generates logs for the following events. Note that logs are generated when an MQTT or HTTP request is received from the device.

Get Job Execution Logs
The AWS IoT Jobs service generates a `GetJobExecution` log when the service receives a job execution request.

For example:

```json
{
  "timestamp": "2018-06-13 17:45:17.197",
  "logLevel": "DEBUG",
  "accountId": "617544064643",
  "status": "Success",
  "eventType": "GetJobExecution",
  "protocol": "MQTT",
  "clientId": "299966ad-54de-40b4-99d3-4fc8b52da0c5",
  "topicName": "$aws/things/299966ad-54de-40b4-99d3-4fc8b52da0c5/jobs/get",
  "clientToken": "24b9a741-15a7-44fc-bd3c-1ff2e34e5e82",
  "details": "The request status is SUCCESS."
}
```

In addition to the attributes common to all CloudWatch Logs, `GetJobExecution` log entries contain the following attributes:

- **eventType**
  - `GetJobExecution` for get job execution logs.

- **protocol**
  - The protocol used when making the request. Valid values are `MQTT` or `HTTP`.

- **clientId**
  - The ID of the client making the request.

- **topicName**
  - The name of the subscribed topic.

- **clientToken**
  - A unique, case-sensitive, identifier to ensure the idempotency of the request. For more information, see [How to Ensure Idempotency](#).

- **details**
  - Additional information from the Jobs service.

Describe Job Execution Logs
The AWS IoT Jobs service generates a `DescribeJobExecution` log when the service receives a request to describe a job execution.
more info (14)

For example:

```json
{
    "timestamp": "2017-08-10 19:13:22.841",
    "logLevel": "DEBUG",
    "accountId": "123456789012",
    "status": "Success",
    "eventType": "DescribeJobExecution",
    "protocol": "MQTT",
    "clientId": "thingOne",
    "jobId": "002",
    "topicName": ":aws/things/thingOne/jobs/002/get",
    "clientToken": "myToken",
    "details": "The request status is SUCCESS."
}
```

In addition to the attributes common to all CloudWatch Logs, GetJobExecution log entries contain the following attributes:

- **eventType**
  - `DescribeJobExecution` for describe job execution logs.

- **protocol**
  - The protocol used when making the request. Valid values are `MQTT` or `HTTP`.

- **clientId**
  - The ID of the client making the request.

- **jobId**
  - The job ID for the job execution.

- **topicName**
  - The topic used to make the request.

- **clientToken**
  - A unique, case-sensitive, identifier to ensure the idempotency of the request. For more information, see How to Ensure Idempotency.

- **details**
  - Additional information from the Jobs service.

**Update Job Execution Logs**

The AWS IoT Jobs service generates an `UpdateJobExecution` log when the service receives a request to update a job execution.

more info (15)

For example:

```json
{
    "timestamp": "2017-08-10 19:25:14.758",
    "logLevel": "DEBUG",
    "accountId": "123456789012",
    "status": "Success",
```
"eventType": "UpdateJobExecution",
"protocol": "MQTT",
"clientId": "thingOne",
"jobId": "002",
"topicName": "$aws/things/thingOne/jobs/002/update",
"clientToken": "myClientToken",
"versionNumber": "1",
"details": "The destination status is IN_PROGRESS. The request status is SUCCESS."
}

In addition to the attributes common to all CloudWatch Logs, UpdateJobExecution log entries contain the following attributes:

**eventType**

UpdateJobExecution for update job execution logs.

**protocol**

The protocol used when making the request. Valid values are MQTT or HTTP.

**clientId**

The ID of the client making the request.

**jobId**

The job ID for the job execution.

**topicName**

The topic used to make the request.

**clientToken**

A unique, case-sensitive, identifier to ensure the idempotency of the request. For more information, see [How to Ensure Idempotency](#).

**versionNumber**

The version of the job execution.

**details**

Additional information from the Jobs service.

Start Next Pending Job Execution Logs

The AWS IoT Jobs service generates a StartNextPendingJobExecution log when the service receives a request to start the next pending job execution.

For example:

```json
{
  "timestamp": "2018-06-13 17:49:51.036",
  "logLevel": "DEBUG",
  "accountId": "617544064643",
  "status": "Success",
  "eventType": "StartNextPendingJobExecution",
  "protocol": "MQTT",
  "clientId": "95c47808-b1ca-4794-bc68-a588d69216c",
  "topicName": "$aws/things/95c47808-b1ca-4794-bc68-a588d69216c/jobs/start-next",
  "clientToken": "bd7447c4-3a05-49f4-8517-dd89b2c68d94",
```
"details": "The request status is SUCCESS."
}

In addition to the attributes common to all CloudWatch Logs, StartNextPendingJobExecution log entries contain the following attributes:

**eventType**

StartNextPendingJobExecution for start next pending job execution logs.

**protocol**

The protocol used when making the request. Valid values are MQTT or HTTP.

**clientId**

The ID of the client making the request.

**topicName**

The topic used to make the request.

**clientToken**

A unique, case-sensitive, identifier to ensure the idempotency of the request. For more information, see How to Ensure Idempotency.

**details**

Additional information from the Jobs service.

### Report Final Job Execution Count Logs

The AWS IoT Jobs service generates a ReportFinalJobExecutionCount log when a job is completed.

For example:

```json
{
  "timestamp": "2017-08-10 19:44:16.776",
  "logLevel": "INFO",
  "accountId": "123456789012",
  "status": "Success",
  "eventType": "ReportFinalJobExecutionCount",
  "protocol": "MQTT",
  "jobId": "002",
  "details": "Job 002 completed. QUEUED job execution count: 0 IN_PROGRESS job execution count: 0 FAILED job execution count: 0 SUCCESS job execution count: 1 CANCELED job execution count: 0 REJECTED job execution count: 0 REMOVED job execution count: 0"
}
```

In addition to the attributes common to all CloudWatch Logs, ReportFinalJobExecutionCount log entries contain the following attributes:

**eventType**

ReportFinalJobExecutionCount for report final job execution count logs.

**protocol**

The protocol used when making the request. The valid value is MQTT (not HTTP).
jobId

The job ID for the job execution.

details

Additional information from the Jobs service.

Viewing Logs

To view your logs

2. In the Filter text box, type AWSIoTLogsV2, and press Enter.
3. Double-click the AWSIoTLogsV2 log group.
4. Choose Search Log Group. A complete list of the AWS IoT logs generated for your account is displayed.
5. Choose the expand icon to look at an individual stream.

You can also type a query in the Filter events text box. Here are some interesting queries to try:

- `{ $.logLevel = "INFO" }`
  Find all logs that have a log level of INFO.
- `{ $.status = "Success" }`
  Find all logs that have a status of Success.
- `{ $.status = "Success" && $.eventType = "GetThingShadow" }`
  Find all logs that have a status of Success and an event type of GetThingShadow.

For more information about creating filter expressions, see CloudWatch Logs Queries.

Diagnosing Rules Issues

CloudWatch Logs is the best place to debug issues you are having with rules. When you enable CloudWatch Logs for AWS IoT, you can see which rules are triggered and their success or failure. You also get information about whether WHERE clause conditions match.

The most common rules issue is authorization. The logs show if your role is not authorized to perform AssumeRole on the resource. Here is an example log generated by fine-grained logging (p. 555):

```json
{
    "timestamp": "2017-12-09 22:49:17.954",
    "logLevel": "ERROR",
    "traceId": "ff563525-6469-506a-e141-78d40375fc4e",
    "accountId": "123456789012",
    "status": "Failure",
    "eventType": "RuleExecution",
    "clientId": "iotconsole-123456789012-3",
    "topicName": "test-topic",
    "ruleName": "rule1",
    "ruleAction": "DynamoAction",
    "resources": {
        "ItemHashKeyField": "id",
    }
}
```
Diagnosing Problems with Shadows

Diagnosing Shadows

<table>
<thead>
<tr>
<th>Issue</th>
<th>Troubleshooting Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>A device's shadow document is rejected with &quot;Invalid JSON document.&quot;</td>
<td>If you are unfamiliar with JSON, modify the examples provided in this guide for your own use. For more information, see Device Shadow Document Syntax.</td>
</tr>
<tr>
<td>I submitted correct JSON, but none or only parts of it are stored in the device's shadow document.</td>
<td>Be sure you are following the JSON formatting guidelines. Only JSON fields in the desired and reported sections are stored. JSON content (even if formally correct) outside of those sections is ignored.</td>
</tr>
<tr>
<td>I received an error that the device's shadow exceeds the allowed size.</td>
<td>The device's shadow supports 8 KB of data only. Try shortening field names inside of your JSON document or simply create more shadows by creating more things. A device can have an unlimited number of things/shadows associated with it. The only requirement is that each thing name must be unique in your account.</td>
</tr>
</tbody>
</table>

For more information, see the section called “Viewing Logs” (p. 570).

External services are controlled by the end user. Before rule execution, make sure external services are set up with enough throughput and capacity units.
## Issue

<table>
<thead>
<tr>
<th>Issue</th>
<th>Troubleshooting Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>When I receive a device's shadow, it is larger than 8 KB. How can this happen?</td>
<td>Upon receipt, the AWS IoT service adds metadata to the device's shadow. The service includes this data in its response, but it does not count toward the limit of 8 KB. Only the data for desired and reported state inside the state document sent to the device's shadow counts toward the limit.</td>
</tr>
<tr>
<td>My request has been rejected due to incorrect version. What should I do?</td>
<td>Perform a GET operation to sync to the latest state document version. When using MQTT, subscribe to the ./update/accepted topic to be notified about state changes and receive the latest version of the JSON document.</td>
</tr>
<tr>
<td>The timestamp is off by several seconds.</td>
<td>The timestamp for individual fields and the whole JSON document is updated when the document is received by the AWS IoT service or when the state document is published onto the ./update/accepted and ./update/delta message. Messages can be delayed over the network, which can cause the timestamp to be off by a few seconds.</td>
</tr>
<tr>
<td>My device can publish and subscribe on the corresponding shadow topics, but when I attempt to update the shadow document over the HTTP REST API, I get HTTP 403.</td>
<td>Be sure you have created policies in IAM to allow access to these topics and for the corresponding action (UPDATE/GET/DELETE) for the credentials you are using. IAM policies and certificate policies are independent.</td>
</tr>
<tr>
<td>Other issues.</td>
<td>The Device Shadow service logs errors to CloudWatch Logs. To identify device and configuration issues, enable CloudWatch Logs and view the logs for debug information.</td>
</tr>
</tbody>
</table>

## Diagnosing Salesforce IoT Input Stream Action Issues

### Execution Trace

How do I see the execution trace of a Salesforce action?

If CloudWatch Logs are not set up, see the **Setting Up CloudWatch Logs with AWS IoT (p. 552)** section. After you have activated the logs, you are able to see the execution trace of the Salesforce action.

### Action Success and Failure

How do I check that messages have been sent successfully to a Salesforce IoT input stream?

View the logs generated by execution of the Salesforce action in CloudWatch Logs. If you see "Action executed successfully," then it means that the AWS IoT rules engine received confirmation from the Salesforce IoT that the message was successfully pushed to the targeted input stream.
If you are experiencing problems with the Salesforce IoT platform, contact Salesforce IoT support.

What do I do if messages have not been sent successfully to a Salesforce IoT input stream?

View the logs generated by execution of the Salesforce action in CloudWatch Logs. Depending on the log entry, you can try the following actions:

Failed to locate the host

Check that the url parameter of the action is correct and that your Salesforce IoT input stream exists.

Received Internal Server Error from Salesforce

Retry. If the problem persists, contact Salesforce IoT Support.

Received Bad Request Exception from Salesforce

Check the payload you are sending for errors.

Received Unsupported Media Type Exception from Salesforce

Salesforce IoT does not support a binary payload at this time. Check that you are sending a JSON payload.

Received Unauthorized Exception from Salesforce

Check that the token parameter of the action is correct and that your token is still valid.

Received Not Found Exception from Salesforce

Check that the url parameter of the action is correct and that your Salesforce IoT input stream exists.

If you receive an error that is not listed here, contact AWS Support.

AWS IoT Limits

AWS IoT limit information and values are provided in the AWS IoT Limits section of the Amazon Web Services General Reference.

AWS IoT Errors

This section lists the error codes sent by AWS IoT.

Message Broker Error Codes

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Error Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>Bad request.</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized.</td>
</tr>
<tr>
<td>403</td>
<td>Forbidden.</td>
</tr>
<tr>
<td>503</td>
<td>Service unavailable.</td>
</tr>
</tbody>
</table>

Identity and Security Error Codes

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Error Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>401</td>
<td>Unauthorized.</td>
</tr>
</tbody>
</table>
## Device Shadow Error Codes

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Error Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>Bad request.</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized.</td>
</tr>
<tr>
<td>403</td>
<td>Forbidden.</td>
</tr>
<tr>
<td>404</td>
<td>Not found.</td>
</tr>
<tr>
<td>409</td>
<td>Conflict.</td>
</tr>
<tr>
<td>413</td>
<td>Request too large.</td>
</tr>
<tr>
<td>422</td>
<td>Failed to process request.</td>
</tr>
<tr>
<td>429</td>
<td>Too many requests.</td>
</tr>
<tr>
<td>500</td>
<td>Internal error.</td>
</tr>
<tr>
<td>503</td>
<td>Service unavailable.</td>
</tr>
</tbody>
</table>
IOT Commands

This chapter contains the following sections:

- AcceptCertificateTransfer (p. 579)
- AddThingToThingGroup (p. 581)
- AssociateTargetsWithJob (p. 583)
- AttachPolicy (p. 587)
- AttachPrincipalPolicy (p. 589)
- AttachSecurityProfile (p. 591)
- AttachThingPrincipal (p. 594)
- CancelAuditTask (p. 596)
- CancelCertificateTransfer (p. 597)
- CancelJob (p. 599)
- CancelJobExecution (p. 603)
- ClearDefaultAuthorizer (p. 607)
- CreateAuthorizer (p. 609)
- CreateCertificateFromCsr (p. 612)
- CreateJob (p. 616)
- CreateKeysAndCertificate (p. 621)
- CreateOTAUpdate (p. 624)
- CreatePolicy (p. 631)
- CreatePolicyVersion (p. 635)
- CreateRoleAlias (p. 639)
- CreateScheduledAudit (p. 642)
- CreateSecurityProfile (p. 646)
- CreateStream (p. 651)
- CreateThing (p. 655)
- CreateThingGroup (p. 659)
- CreateThingType (p. 663)
- CreateTopicRule (p. 666)
- DeleteAccountAuditConfiguration (p. 684)
- DeleteAuthorizer (p. 686)
- DeleteCACertificate (p. 688)
- DeleteCertificate (p. 690)
- DeleteJob (p. 692)
- DeleteJobExecution (p. 695)
- DeleteOTAUpdate (p. 699)
• DeletePolicy (p. 701)
• DeletePolicyVersion (p. 703)
• DeleteRegistrationCode (p. 705)
• DeleteRoleAlias (p. 706)
• DeleteScheduledAudit (p. 708)
• DeleteSecurityProfile (p. 710)
• DeleteStream (p. 712)
• DeleteThing (p. 714)
• DeleteThingGroup (p. 716)
• DeleteThingShadow (p. 718)
• DeleteThingType (p. 721)
• DeleteTopicRule (p. 723)
• DeleteV2LoggingLevel (p. 724)
• DeprecateThingType (p. 726)
• DescribeAccountAuditConfiguration (p. 728)
• DescribeAuditTask (p. 731)
• DescribeAuthorizer (p. 735)
• DescribeCACertificate (p. 739)
• DescribeCertificate (p. 743)
• DescribeDefaultAuthorizer (p. 747)
• DescribeEndpoint (p. 750)
• DescribeEventConfigurations (p. 752)
• DescribeIndex (p. 754)
• DescribeJob (p. 757)
• DescribeJobExecution (p. 762)
• DescribeRoleAlias (p. 771)
• DescribeScheduledAudit (p. 774)
• DescribeSecurityProfile (p. 777)
• DescribeStream (p. 782)
• DescribeThing (p. 786)
• DescribeThingGroup (p. 790)
• DescribeThingRegistrationTask (p. 794)
• DescribeThingType (p. 798)
• DetachPolicy (p. 801)
• DetachPrincipalPolicy (p. 804)
• DetachSecurityProfile (p. 806)
• DetachThingPrincipal (p. 808)
• DisableTopicRule (p. 810)
• EnableTopicRule (p. 812)
• GetEffectivePolicies (p. 813)
• GetIndexingConfiguration (p. 816)
• GetJobDocument (p. 819)
• GetLoggingOptions (p. 821)
• GetOTAUpdate (p. 822)
• GetPendingJobExecutions (p. 829)
• GetPolicy (p. 833)
• GetPolicyVersion (p. 836)
• GetRegistrationCode (p. 839)
• GetThingShadow (p. 841)
• GetTopicRule (p. 844)
• GetV2LoggingOptions (p. 862)
• ListActiveViolations (p. 864)
• ListAttachedPolicies (p. 869)
• ListAuditFindings (p. 872)
• ListAuditTasks (p. 881)
• ListAuthorizers (p. 885)
• ListCACertificates (p. 888)
• ListCertificates (p. 891)
• ListCertificatesByCA (p. 894)
• ListIndices (p. 898)
• ListJobExecutionsForJob (p. 901)
• ListJobExecutionsForThing (p. 905)
• ListJobs (p. 908)
• ListOTAUpdates (p. 913)
• ListOutgoingCertificates (p. 916)
• ListPolicies (p. 920)
• ListPolicyPrincipals (p. 923)
• ListPolicyVersions (p. 926)
• ListPrincipalPolicies (p. 929)
• ListPrincipalThings (p. 932)
• ListRoleAliases (p. 935)
• ListScheduledAudits (p. 938)
• ListSecurityProfiles (p. 941)
• ListSecurityProfilesForTarget (p. 944)
• ListStreams (p. 947)
• ListTargetsForPolicy (p. 950)
• ListTargetsForSecurityProfile (p. 953)
• ListThingGroups (p. 956)
• ListThingGroupsForThing (p. 960)
• ListThingPrincipals (p. 963)
• ListThingRegistrationTaskReports (p. 965)
• ListThingRegistrationTasks (p. 968)
• ListThingTypes (p. 971)
• ListThings (p. 975)
• ListThingsInThingGroup (p. 978)
• ListTopicRules (p. 981)
• ListV2LoggingLevels (p. 984)
• ListViolationEvents (p. 987)
• Publish (p. 993)
• RegisterCACertificate (p. 995)
• RegisterCertificate (p. 999)
• RegisterThing (p. 1003)
• RejectCertificateTransfer (p. 1006)
• RemoveThingFromThingGroup (p. 1009)
• ReplaceTopicRule (p. 1011)
• SearchIndex (p. 1028)
• SetDefaultAuthorizer (p. 1033)
• SetDefaultPolicyVersion (p. 1035)
• SetLoggingOptions (p. 1037)
• SetV2LoggingLevel (p. 1039)
• SetV2LoggingOptions (p. 1041)
• StartNextPendingJobExecution (p. 1043)
• StartOnDemandAuditTask (p. 1047)
• StartThingRegistrationTask (p. 1050)
• StopThingRegistrationTask (p. 1052)
• TestAuthorization (p. 1054)
• TestInvokeAuthorizer (p. 1061)
• TransferCertificate (p. 1065)
• UpdateAccountAuditConfiguration (p. 1068)
• UpdateAuthorizer (p. 1072)
• UpdateCACertificate (p. 1075)
• UpdateCertificate (p. 1078)
• UpdateEventConfigurations (p. 1081)
• UpdateIndexingConfiguration (p. 1083)
• UpdateJobExecution (p. 1085)
• UpdateRoleAlias (p. 1091)
• UpdateScheduledAudit (p. 1094)
• UpdateSecurityProfile (p. 1098)
• UpdateStream (p. 1106)
• UpdateThing (p. 1110)
• UpdateThingGroup (p. 1114)
• UpdateThingGroupsForThing (p. 1117)
AcceptCertificateTransfer

Accepts a pending certificate transfer. The default state of the certificate is INACTIVE.

To check for pending certificate transfers, call ListCertificates to enumerate your certificates.

**https**

**Request syntax:**

```
PATCH /accept-certificate-transfer/certificateId?setAsActive=setAsActive
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>CertificateId</td>
<td>yes</td>
<td>The ID of the certificate. (The last part of the certificate ARN contains the certificate ID.)</td>
</tr>
<tr>
<td>setAsActive</td>
<td>SetAsActive</td>
<td>no</td>
<td>Specifies whether the certificate is active.</td>
</tr>
</tbody>
</table>

**Errors:**

- **ResourceNotFoundException**
  
  The specified resource does not exist.
  
  HTTP response code: 404

- **TransferAlreadyCompletedException**
  
  You can't revert the certificate transfer because the transfer is already complete.
  
  HTTP response code: 410

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  
  HTTP response code: 400

- **ThrottlingException**
  
  The rate exceeds the limit.
  
  HTTP response code: 429
UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```bash
aws iot accept-certificate-transfer \
   --certificate-id <value> \
   [--set-as-active | --no-set-as-active] \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
   "certificateId": "string",
   "setAsActive": "boolean"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>string</td>
<td>The ID of the certificate. (The last part of the certificate ARN contains the certificate ID.)</td>
</tr>
<tr>
<td></td>
<td>length: max:64 min:64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: (0x)?[a-fA-F0-9]+</td>
<td></td>
</tr>
<tr>
<td>setAsActive</td>
<td>boolean</td>
<td>Specifies whether the certificate is active.</td>
</tr>
</tbody>
</table>

Output:

None

Errors:

ResourceNotFoundException

The specified resource does not exist.
TransferAlreadyCompletedException

You can't revert the certificate transfer because the transfer is already complete.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

AddThingToThingGroup

Adds a thing to a thing group.

https

Request syntax:

```
PUT /thing-groups/addThingToThingGroup
Content-type: application/json

{
  "thingGroupName": "string",
  "thingGroupArn": "string",
  "thingName": "string",
  "thingArn": "string"
}
```

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>ThingGroupName</td>
<td>no</td>
<td>The name of the group to which you are adding a thing.</td>
</tr>
<tr>
<td>thingGroupArn</td>
<td>ThingGroupArn</td>
<td>no</td>
<td>The ARN of the group to which you are adding a thing.</td>
</tr>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>no</td>
<td>The name of the thing to add to a group.</td>
</tr>
</tbody>
</table>
AddThingToThingGroup

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingArn</td>
<td>ThingArn</td>
<td>no</td>
<td>The ARN of the thing to add to a group.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404

**cli**

**Synopsis:**

```bash
aws iot add-thing-to-thing-group \
    [--thing-group-name <value>] \
    [--thing-group-arn <value>] \
    [--thing-name <value>] \
    [--thing-arn <value>] \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
    "thingGroupName": "string",
    "thingGroupArn": "string",
    "thingName": "string",
    "thingArn": "string"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>string</td>
<td>The name of the group to which you are adding a thing.</td>
</tr>
</tbody>
</table>
AssociateTargetsWithJob

Associates a group with a continuous job. The following criteria must be met:

- The job must have been created with the targetSelection field set to "CONTINUOUS".
- The job status must currently be "IN_PROGRESS".
- The total number of targets associated with a job must not exceed 100.

### Output:

None

### Errors:

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ThrottlingException**
  
  The rate exceeds the limit.

- **InternalFailureException**
  
  An unexpected error has occurred.

- **ResourceNotFoundException**
  
  The specified resource does not exist.

### Request syntax:

```plaintext
POST /jobs/jobId/targets
```
Content-type: application/json

{
  "targets": [
    "string"
  ],
  "comment": "string"
}

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobld</td>
<td>JobId</td>
<td>yes</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targets</td>
<td>JobTargets</td>
<td>yes</td>
<td>A list of thing group ARNs that define the targets of the job.</td>
</tr>
<tr>
<td>comment</td>
<td>Comment</td>
<td>no</td>
<td>An optional comment string describing why the job was associated with the targets.</td>
</tr>
</tbody>
</table>

**Response syntax:**

Content-type: application/json

{
  "jobArn": "string",
  "jobId": "string",
  "description": "string"
}

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobArn</td>
<td>JobArn</td>
<td>no</td>
<td>An ARN identifying the job.</td>
</tr>
<tr>
<td>jobld</td>
<td>JobId</td>
<td>no</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td>description</td>
<td>JobDescription</td>
<td>no</td>
<td>A short text description of the job.</td>
</tr>
</tbody>
</table>

**Errors:**
**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404

**LimitExceededException**

A limit has been exceeded.

HTTP response code: 410

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**ServiceUnavailableException**

The service is temporarily unavailable.

HTTP response code: 503

---

### cli

**Synopsis:**

```bash
aws iot associate-targets-with-job 
--targets <value> 
--job-id <value> 
[--comment <value>] 
[--cli-input-json <value>] 
[--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
  "targets": [
    "string"
  ],
  "jobId": "string",
  "comment": "string"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targets</td>
<td>list</td>
<td>A list of thing group ARNs that define the targets of the job.</td>
</tr>
<tr>
<td></td>
<td>member: TargetArn</td>
<td></td>
</tr>
</tbody>
</table>
### AssociateTargetsWithJob

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td>length- max:64 min:1</td>
<td>pattern: [a-zA-Z0-9_-]+</td>
<td></td>
</tr>
<tr>
<td>comment</td>
<td>string</td>
<td>An optional comment string describing why the job was associated with the targets.</td>
</tr>
<tr>
<td>length- max:2028</td>
<td>pattern: [^\p{C}]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
  "jobArn": "string",
  "jobId": "string",
  "description": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobArn</td>
<td>string</td>
<td>An ARN identifying the job.</td>
</tr>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td>length- max:64 min:1</td>
<td>pattern: [a-zA-Z0-9_-]+</td>
<td></td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>A short text description of the job.</td>
</tr>
<tr>
<td>length- max:2028</td>
<td>pattern: [^\p{C}]+</td>
<td></td>
</tr>
</tbody>
</table>

**Errors:**

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an `UpdateJobExecution` request contains invalid status details. The message contains details about the error.

- **ResourceNotFoundException**
  
  The specified resource does not exist.

- **LimitExceededException**
  
  A limit has been exceeded.

- **ThrottlingException**
  
  The rate exceeds the limit.
ServiceUnavailableException

The service is temporarily unavailable.

AttachPolicy

Attaches a policy to the specified target.

https

Request syntax:

```plaintext
PUT /target-policies/policyName
Content-type: application/json

{
    "target": "string"
}
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>yes</td>
<td>The name of the policy to attach.</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>PolicyTarget</td>
<td>yes</td>
<td>The identity to which the policy is attached.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429
UnauthorizedException
   You are not authorized to perform this operation.
   HTTP response code: 401
ServiceUnavailableException
   The service is temporarily unavailable.
   HTTP response code: 503
InternalFailureException
   An unexpected error has occurred.
   HTTP response code: 500
LimitExceededException
   A limit has been exceeded.
   HTTP response code: 410

cli

Synopsis:

    aws iot attach-policy \
      --policy-name <value> \
      --target <value>  \
      [--cli-input-json <value>] \
      [--generate-cli-skeleton]

cli-input-json format:

    {
      "policyName": "string",
      "target": "string"
    }

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>string</td>
<td>The name of the policy to attach.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w+=,.@-]+</td>
<td></td>
</tr>
<tr>
<td>target</td>
<td>string</td>
<td>The identity to which the policy is attached.</td>
</tr>
</tbody>
</table>

Output:

None

Errors:
ResourceNotFoundException

The specified resource does not exist.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

LimitExceededException

A limit has been exceeded.

---

AttachPrincipalPolicy

Attaches the specified policy to the specified principal (certificate or other credential).

**Note:** This API is deprecated. Please use AttachPolicy instead.

https

**Request syntax:**

```
PUT /principal-policies/policyName
x-amzn-iot-principal: principal
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>yes</td>
<td>The policy name.</td>
</tr>
<tr>
<td>principal</td>
<td>Principal</td>
<td>yes</td>
<td>The principal, which can be a certificate ARN (as returned from the CreateCertificate operation) or an Amazon Cognito ID.</td>
</tr>
</tbody>
</table>

**Errors:**
ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

LimitExceededException

A limit has been exceeded.

HTTP response code: 410

cli

Synopsis:

```sh
aws iot attach-principal-policy \    
  --policy-name <value> \    
  --principal <value> \    
  [--cli-input-json <value>] \    
  [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "policyName": "string",
  "principal": "string"
}
```
cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [w+,.@-]+</td>
<td></td>
</tr>
<tr>
<td>principal</td>
<td>string</td>
<td>The principal, which can be a certificate ARN (as returned from the CreateCertificate operation) or an Amazon Cognito ID.</td>
</tr>
</tbody>
</table>

Output:

None

Errors:

ResourceNotFoundException

The specified resource does not exist.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

LimitExceeded Exception

A limit has been exceeded.

**AttachSecurityProfile**

Associates a Device Defender security profile with a thing group or with this account. Each thing group or account can have up to five security profiles associated with it.

https

Request syntax:
PUT /security-profiles/{securityProfileName}/targets?
securityProfileTargetArn={securityProfileTargetArn}

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>yes</td>
<td>The security profile that is attached.</td>
</tr>
<tr>
<td>securityProfileTargetArn</td>
<td>SecurityProfileTargetArn</td>
<td>yes</td>
<td>The ARN of the target (thing group) to which the security profile is attached.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404

**LimitExceededException**

A limit has been exceeded.

HTTP response code: 410

**VersionConflictException**

An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

HTTP response code: 409

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

**Synopsis:**
aws iot attach-security-profile
   --security-profile-name <value> \
   --security-profile-target-arn <value> \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]

cli-input-json format:

{
   "securityProfileName": "string",
   "securityProfileTargetArn": "string"
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9:-_]+ The security profile that is attached.</td>
</tr>
<tr>
<td>securityProfileTargetArn</td>
<td>string</td>
<td>The ARN of the target (thing group) to which the security profile is attached.</td>
</tr>
</tbody>
</table>

Output:

None

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceNotFoundException

The specified resource does not exist.

LimitExceededException

A limit has been exceeded.

VersionConflictException

An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.
**AttachThingPrincipal**

Attaches the specified principal to the specified thing.

**https**

**Request syntax:**

```
PUT /things/thingName/principals
x-amzn-principal: principal
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing.</td>
</tr>
<tr>
<td>principal</td>
<td>Principal</td>
<td>yes</td>
<td>The principal, such as a certificate or other credential.</td>
</tr>
</tbody>
</table>

**Errors:**

- **ResourceNotFoundException**
  - The specified resource does not exist.
  - HTTP response code: 404

- **InvalidRequestException**
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  - HTTP response code: 400

- **ThrottlingException**
  - The rate exceeds the limit.
  - HTTP response code: 429

- **UnauthorizedException**
  - You are not authorized to perform this operation.
  - HTTP response code: 401

- **ServiceUnavailableException**
  - The service is temporarily unavailable.
  - HTTP response code: 503

- **InternalFailureException**
  - An unexpected error has occurred.
  - HTTP response code: 500
cli

Synopsis:

```
aws iot attach-thing-principal \
  --thing-name <value> \
  --principal <value> \ 
  [--cli-input-json <value>] \ 
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "thingName": "string",
  "principal": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>principal</td>
<td>string</td>
<td>The principal, such as a certificate or other credential.</td>
</tr>
</tbody>
</table>

Output:

None

Errors:

- **ResourceNotFoundException**
  - The specified resource does not exist.
- **InvalidRequestException**
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
- **ThrottlingException**
  - The rate exceeds the limit.
- **UnauthorizedException**
  - You are not authorized to perform this operation.
- **ServiceUnavailableException**
  - The service is temporarily unavailable.
- **InternalFailureException**
  - An unexpected error has occurred.
CancelAuditTask

Cancels an audit that is in progress. The audit can be either scheduled or on-demand. If the audit is not in progress, an "InvalidRequestException" occurs.

**https**

**Request syntax:**

```
PUT /audit/tasks/taskId/cancel
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>AuditTaskId</td>
<td>yes</td>
<td>The ID of the audit you want to cancel. You can only cancel an audit that is &quot;IN_PROGRESS&quot;.</td>
</tr>
</tbody>
</table>

**Errors:**

- **ResourceNotFoundException**
  
  The specified resource does not exist.
  
  HTTP response code: 404

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  
  HTTP response code: 400

- **ThrottlingException**
  
  The rate exceeds the limit.
  
  HTTP response code: 429

- **InternalFailureException**
  
  An unexpected error has occurred.
  
  HTTP response code: 500

**cli**

**Synopsis:**

```
aws iot cancel-audit-task \
  --task-id <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```
cli-input-json format:

```json
{
  "taskId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>string</td>
<td>The ID of the audit you want to cancel. You can only cancel an audit that is &quot;IN_PROGRESS&quot;.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>string</td>
<td></td>
</tr>
</tbody>
</table>

length- max:40 min:1
pattern: [a-zA-Z0-9-]+

Output:
None

Errors:

ResourceNotFoundException

The specified resource does not exist.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

---

**CancelCertificateTransfer**

Cancels a pending transfer for the specified certificate.

**Note** Only the transfer source account can use this operation to cancel a transfer. (Transfer destinations can use RejectCertificateTransfer instead.) After transfer, AWS IoT returns the certificate to the source account in the INACTIVE state. After the destination account has accepted the transfer, the transfer cannot be cancelled.

After a certificate transfer is cancelled, the status of the certificate changes from PENDING_TRANSFER to INACTIVE.

https

Request syntax:

```bash
PATCH /cancel-certificate-transfer/certificateId
```
URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>CertificateId</td>
<td>yes</td>
<td>The ID of the certificate. (The last part of the certificate ARN contains the certificate ID.)</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

TransferAlreadyCompletedException

You can't revert the certificate transfer because the transfer is already complete.

HTTP response code: 410

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```bash
aws iot cancel-certificate-transfer \   
```
---certificate-id <value>  
[--cli-input-json <value>]  
[--generate-cli-skeleton]

cli-input-json format:

{
  "certificateId": "string"
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>string</td>
<td>The ID of the certificate. (The last part of the certificate ARN contains the certificate ID.) length= max:64 min:64 pattern: (0x)?[a-fA-F0-9]+</td>
</tr>
</tbody>
</table>

Output:
None

Errors:

ResourceNotFoundException
   The specified resource does not exist.
TransferAlreadyCompletedException
   You can't revert the certificate transfer because the transfer is already complete.
InvalidRequestException
   The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
ThrottlingException
   The rate exceeds the limit.
UnauthorizedException
   You are not authorized to perform this operation.
ServiceUnavaibleException
   The service is temporarily unavailable.
InternalFailureException
   An unexpected error has occurred.

CancelJob

Cancels a job.
**https**

**Request syntax:**

```
PUT /jobs/jobId/cancel?force=force
Content-type: application/json

{
   "comment": "string"
}
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>JobId</td>
<td>yes</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td>force</td>
<td>ForceFlag</td>
<td>no</td>
<td>(Optional) If true job executions with status &quot;IN_PROGRESS&quot; and &quot;QUEUED&quot; are canceled, otherwise only job executions with status &quot;QUEUED&quot; are canceled. The default is false. Canceling a job which is &quot;IN_PROGRESS&quot;, will cause a device which is executing the job to be unable to update the job execution status. Use caution and ensure that each device executing a job which is canceled is able to recover to a valid state.</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>comment</td>
<td>Comment</td>
<td>no</td>
<td>An optional comment string describing why the job was canceled.</td>
</tr>
</tbody>
</table>

**Response syntax:**

```
Content-type: application/json

{
   "jobArn": "string",
   "jobId": "string",
   "status": "CANCELED"
}
```
"description": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobArn</td>
<td>JobArn</td>
<td>no</td>
<td>The job ARN.</td>
</tr>
<tr>
<td>jobId</td>
<td>JobId</td>
<td>no</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td>description</td>
<td>JobDescription</td>
<td>no</td>
<td>A short text description of the job.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

cli

Synopsis:

aws iot cancel-job \
   --job-id <value> \ 
   [--comment <value>] \ 
   [--force | --no-force] \ 
   [--cli-input-json <value>] \ 
   [--generate-cli-skeleton]

cli-input-json format:

{
   "jobId": "string",
   "comment": "string",
   "force": "boolean"
**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td>comment</td>
<td>string</td>
<td>An optional comment string describing why the job was canceled.</td>
</tr>
<tr>
<td>force</td>
<td>boolean</td>
<td>(Optional) If true job executions with status &quot;IN_PROGRESS&quot; and &quot;QUEUED&quot; are canceled, otherwise only job executions with status &quot;QUEUED&quot; are canceled. The default is false. Canceling a job which is &quot;IN_PROGRESS&quot;, will cause a device which is executing the job to be unable to update the job execution status. Use caution and ensure that each device executing a job which is canceled is able to recover to a valid state.</td>
</tr>
</tbody>
</table>

**Output:**

```json
{
  "jobArn": "string",
  "jobId": "string",
  "description": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobArn</td>
<td>string</td>
<td>The job ARN.</td>
</tr>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>A short text description of the job.</td>
</tr>
</tbody>
</table>
Errors:

InvalidRequestException
   The contents of the request were invalid. For example, this code is returned when an
   UpdateJobExecution request contains invalid status details. The message contains details about the
   error.

ResourceNotFoundException
   The specified resource does not exist.

ThrottlingException
   The rate exceeds the limit.

ServiceUnavailableException
   The service is temporarily unavailable.

CancelJobExecution

Cancels the execution of a job for a given thing.

https

Request syntax:

```
PUT /things/thingName/jobs/jobId/cancel?force=force
Content-type: application/json

{
   "expectedVersion": "long",
   "statusDetails": {
     "string": "string"
   }
}
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>JobId</td>
<td>yes</td>
<td>The ID of the job to be canceled.</td>
</tr>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing whose execution of the job will be canceled.</td>
</tr>
<tr>
<td>force</td>
<td>ForceFlag</td>
<td>no</td>
<td>(Optional) If true the job execution will be canceled if it has status IN_PROGRESS or QUEUED, otherwise the job execution will be canceled only if it has status QUEUED. If you attempt to cancel a job execution that is IN_PROGRESS, and you do not set</td>
</tr>
</tbody>
</table>
### Name

<table>
<thead>
<tr>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>force</strong> to true, then an <strong>InvalidStateTransitionException</strong> will be thrown. The default is <strong>false</strong>. Canceling a job execution which is &quot;IN_PROGRESS&quot;, will cause the device to be unable to update the job execution status. Use caution and ensure that the device is able to recover to a valid state.</td>
</tr>
</tbody>
</table>

### Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>expectedVersion</td>
<td>ExpectedVersion</td>
<td>no</td>
<td>(Optional) The expected current version of the job execution. Each time you update the job execution, its version is incremented. If the version of the job execution stored in Jobs does not match, the update is rejected with a VersionMismatch error, and an ErrorResponse that contains the current job execution status data is returned. (This makes it unnecessary to perform a separate DescribeJobExecution request in order to obtain the job execution status data.)</td>
</tr>
<tr>
<td>statusDetails</td>
<td>DetailsMap</td>
<td>no</td>
<td>A collection of name/value pairs that describe the status of the job execution. If not specified, the statusDetails are unchanged. You can specify at most 10 name/value pairs.</td>
</tr>
</tbody>
</table>

### Errors:

604
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

InvalidStateTransitionException

An update attempted to change the job execution to a state that is invalid because of the job execution's current state (for example, an attempt to change a request in state SUCCESS to state IN_PROGRESS). In this case, the body of the error message also contains the executionState field.

HTTP response code: 409

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

VersionConflictException

An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

HTTP response code: 409

cli

Synopsis:

aws iot cancel-job-execution \ 
  --job-id <value> \ 
  --thing-name <value> \ 
  [--force | --no-force] \ 
  [--expected-version <value>] \ 
  [--status-details <value>] \ 
  [--cli-input-json <value>] \ 
  [--generate-cli-skeleton]

cli-input-json format:

{
  "jobId": "string",
  "thingName": "string",
  "force": "boolean",
  "expectedVersion": "long",
}
"statusDetails": {
    "string": "string"
}

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The ID of the job to be canceled.</td>
</tr>
<tr>
<td></td>
<td>length:</td>
<td>max:64 min:1</td>
</tr>
<tr>
<td></td>
<td>pattern:</td>
<td>[a-zA-Z0-9-_]+</td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing whose execution of the job will be canceled.</td>
</tr>
<tr>
<td></td>
<td>length:</td>
<td>max:128 min:1</td>
</tr>
<tr>
<td></td>
<td>pattern:</td>
<td>[a-zA-Z0-9-_]+</td>
</tr>
<tr>
<td>force</td>
<td>boolean</td>
<td>(Optional) If <strong>true</strong> the job execution will be canceled if it has status IN_PROGRESS or QUEUED, otherwise the job execution will be canceled only if it has status QUEUED. If you attempt to cancel a job execution that is IN_PROGRESS, and you do not set force to <strong>true</strong>, then an <strong>InvalidStateTransitionException</strong> will be thrown. The default is <strong>false</strong>. Canceling a job execution which is &quot;IN_PROGRESS&quot;, will cause the device to be unable to update the job execution status. Use caution and ensure that the device is able to recover to a valid state.</td>
</tr>
<tr>
<td>expectedVersion</td>
<td>long</td>
<td>(Optional) The expected current version of the job execution. Each time you update the job execution, its version is incremented. If the version of the job execution stored in Jobs does not match, the update is rejected with a <strong>VersionMismatch</strong> error, and an <strong>ErrorResponse</strong> that contains the current job execution status data is returned. (This makes it unnecessary to perform a separate <strong>DescribeJobExecution</strong> request in order to obtain the job execution status data.)</td>
</tr>
</tbody>
</table>
ClearDefaultAuthorizer

Clears the default authorizer.

Request syntax:

DELETE /default-authorizer

Errors:

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot clear-default-authorizer \ 
  [--cli-input-json <value>] \ 
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
}
```

Output:

None

Errors:

ResourceNotFoundException

The specified resource does not exist.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.
UnauthorizedException

You are not authorized to perform this operation.
ServiceUnavailableException

The service is temporarily unavailable.
InternalFailureException

An unexpected error has occurred.

CreateAuthorizer

Creates an authorizer.

https

Request syntax:

```
POST /authorizer/authorizerName
Content-type: application/json

{
  "authorizerFunctionArn": "string",
  "tokenKeyName": "string",
  "tokenSigningPublicKeys": {
    "string": "string"
  },
  "status": "string"
}
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>AuthorizerName</td>
<td>yes</td>
<td>The authorizer name.</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerFunctionArn</td>
<td>AuthorizerFunctionArn</td>
<td>yes</td>
<td>The ARN of the authorizer's Lambda function.</td>
</tr>
<tr>
<td>tokenKeyName</td>
<td>TokenKeyName</td>
<td>yes</td>
<td>The name of the token key used to extract the token from the HTTP headers.</td>
</tr>
<tr>
<td>tokenSigningPublicKeys</td>
<td>PublicKeyMap</td>
<td>yes</td>
<td>The public keys used to verify the digital signature returned by your custom authentication service.</td>
</tr>
</tbody>
</table>
CreateAuthorizer

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>AuthorizerStatus</td>
<td>no</td>
<td>The status of the create authorizer request.</td>
</tr>
</tbody>
</table>

**Response syntax:**

```
Content-type: application/json
{
  "authorizerName": "string",
  "authorizerArn": "string"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>AuthorizerName</td>
<td>no</td>
<td>The authorizer’s name.</td>
</tr>
<tr>
<td>authorizerArn</td>
<td>AuthorizerArn</td>
<td>no</td>
<td>The authorizer ARN.</td>
</tr>
</tbody>
</table>

**Errors:**

- **ResourceAlreadyExistsException**
  - The resource already exists.
  - HTTP response code: 409

- **InvalidRequestException**
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  - HTTP response code: 400

- **LimitExceededException**
  - A limit has been exceeded.
  - HTTP response code: 410

- **ThrottlingException**
  - The rate exceeds the limit.
  - HTTP response code: 429

- **UnauthorizedException**
  - You are not authorized to perform this operation.
  - HTTP response code: 401

- **ServiceUnavailableException**
  - The service is temporarily unavailable.
  - HTTP response code: 503
InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

cli

Synopsis:

```
aws iot create-authorizer \
--authorizer-name <value> \
--authorizer-function-arn <value> \
--token-key-name <value> \
--token-signing-public-keys <value> \
[--status <value>]  \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "authorizerName": "string",
  "authorizerFunctionArn": "string",
  "tokenKeyName": "string",
  "tokenSigningPublicKeys": {
    "string": "string"
  },
  "status": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>string</td>
<td>The authorizer name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w=,@-]+</td>
<td></td>
</tr>
<tr>
<td>authorizerFunctionArn</td>
<td>string</td>
<td>The ARN of the authorizer's Lambda function.</td>
</tr>
<tr>
<td>tokenKeyName</td>
<td>string</td>
<td>The name of the token key used to extract the token from the HTTP headers.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9_-]+</td>
<td></td>
</tr>
<tr>
<td>tokenSigningPublicKeys</td>
<td>map</td>
<td>The public keys used to verify the digital signature returned by your custom authentication service.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the create authorizer request.</td>
</tr>
<tr>
<td></td>
<td>enum: ACTIVE</td>
<td>INACTIVE</td>
</tr>
</tbody>
</table>
Output:

```json
{
  "authorizerName": "string",
  "authorizerArn": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>string</td>
<td>The authorizer's name.</td>
</tr>
<tr>
<td>authorizerArn</td>
<td>string</td>
<td>The authorizer ARN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>length- max:128 min:1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pattern: [w=,@-]+</td>
</tr>
</tbody>
</table>

Errors:

ResourceAlreadyExistsException

The resource already exists.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

LimitExceededException

A limit has been exceeded.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

**CreateCertificateFromCsr**

Creates an X.509 certificate using the specified certificate signing request.

**Note:** The CSR must include a public key that is either an RSA key with a length of at least 2048 bits or an ECC key from NIST P-256 or NIST P-384 curves.

**Note:** Reusing the same certificate signing request (CSR) results in a distinct certificate.
You can create multiple certificates in a batch by creating a directory, copying multiple .csr files into that directory, and then specifying that directory on the command line. The following commands show how to create a batch of certificates given a batch of CSRs.

Assuming a set of CSRs are located inside of the directory my-csr-directory:

On Linux and OS X, the command is:

```bash
$ ls my-csr-directory/ | xargs -I  aws iot create-certificate-from-csr --certificate-signing-request file://my-csr-directory/
```

This command lists all of the CSRs in my-csr-directory and pipes each CSR file name to the `aws iot create-certificate-from-csr` AWS CLI command to create a certificate for the corresponding CSR.

The `aws iot create-certificate-from-csr` part of the command can also be run in parallel to speed up the certificate creation process:

```bash
$ ls my-csr-directory/ | xargs -P 10 -I  aws iot create-certificate-from-csr --certificate-signing-request file://my-csr-directory/
```

On Windows PowerShell, the command to create certificates for all CSRs in my-csr-directory is:

```powershell
> ls -Name my-csr-directory | % aws iot create-certificate-from-csr --certificate-signing-request file://my-csr-directory/$_
```

On a Windows command prompt, the command to create certificates for all CSRs in my-csr-directory is:

```cmd
> forfiles /p my-csr-directory /c "cmd /c aws iot create-certificate-from-csr --certificate-signing-request file://@path"
```

https

**Request syntax:**

```
POST /certificates?setAsActive=setAsActive
Content-type: application/json

{
  "certificateSigningRequest": "string"
}
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>setAsActive</td>
<td>SetAsActive</td>
<td>no</td>
<td>Specifies whether the certificate is active.</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateSigningRequest</td>
<td>CertificateSigningRequest</td>
<td>yes</td>
<td>The certificate signing request (CSR).</td>
</tr>
</tbody>
</table>
Content-type: application/json

{
  "certificateArn": "string",
  "certificateId": "string",
  "certificatePem": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateArn</td>
<td>CertificateArn</td>
<td>no</td>
<td>The Amazon Resource Name (ARN) of the certificate. You can use the ARN as a principal for policy operations.</td>
</tr>
<tr>
<td>certificateId</td>
<td>CertificateId</td>
<td>no</td>
<td>The ID of the certificate. Certificate management operations only take a certificateId.</td>
</tr>
<tr>
<td>certificatePem</td>
<td>CertificatePem</td>
<td>no</td>
<td>The certificate data, in PEM format.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500
cli

Synopsis:

```bash
aws iot create-certificate-from-csr \
  --certificate-signing-request <value> \
  [--set-as-active | --no-set-as-active] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "certificateSigningRequest": "string",
  "setAsActive": "boolean"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateSigningRequest</td>
<td>string</td>
<td>The certificate signing request (CSR).</td>
</tr>
<tr>
<td>length- min:1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>setAsActive</td>
<td>boolean</td>
<td>Specifies whether the certificate is active.</td>
</tr>
</tbody>
</table>

Output:

```json
{
  "certificateArn": "string",
  "certificateId": "string",
  "certificatePem": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateArn</td>
<td>string</td>
<td>The Amazon Resource Name (ARN) of the certificate. You can use the ARN as a principal for policy operations.</td>
</tr>
<tr>
<td>certificateId</td>
<td>string length- max:64 min:64 pattern: (0x)?[a-fA-F0-9]+</td>
<td>The ID of the certificate. Certificate management operations only take a certificateId.</td>
</tr>
<tr>
<td>certificatePem</td>
<td>string length- max:65536 min:1</td>
<td>The certificate data, in PEM format.</td>
</tr>
</tbody>
</table>

Errors:
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

CreateJob

Creates a job.

https

Request syntax:

PUT /jobs/jobId
Content-type: application/json

{
  "targets": [
    "string"
  ],
  "documentSource": "string",
  "document": "string",
  "description": "string",
  "presignedUrlConfig": {
    "roleArn": "string",
    "expiresInSec": "long"
  },
  "targetSelection": "string",
  "jobExecutionsRolloutConfig": {
    "maximumPerMinute": "integer"
  }
}

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>JobId</td>
<td>yes</td>
<td>A job identifier which must be unique for your AWS account. We recommend using a UUID. Alpha-numeric</td>
</tr>
</tbody>
</table>
AWS IoT Developer Guide
CreateJob

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>characters, &quot;,&quot; and &quot;_&quot; are valid for use here.</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targets</td>
<td>JobTargets</td>
<td>yes</td>
<td>A list of things and thing groups to which the job should be sent.</td>
</tr>
<tr>
<td>documentSource</td>
<td>JobDocumentSource</td>
<td>no</td>
<td>An S3 link to the job document.</td>
</tr>
<tr>
<td>document</td>
<td>JobDocument</td>
<td>no</td>
<td>The job document.</td>
</tr>
<tr>
<td>description</td>
<td>JobDescription</td>
<td>no</td>
<td>A short text description of the job.</td>
</tr>
<tr>
<td>presignedUrlConfig</td>
<td>PresignedUrlConfig</td>
<td>no</td>
<td>Configuration information for pre-signed S3 URLs.</td>
</tr>
<tr>
<td>targetSelection</td>
<td>TargetSelection</td>
<td>no</td>
<td>Specifies whether the job will continue to run (CONTINUOUS), or will be complete after all those things specified as targets have completed the job (SNAPSHOT). If continuous, the job may also be run on a thing when a change is detected in a target. For example, a job will run on a thing when the thing is added to a target group, even after the job was completed by all things originally in the group.</td>
</tr>
</tbody>
</table>

jobExecutionsRolloutConfig | JobExecutionsRolloutConfig | no | Allows you to create a staged rollout of the job. |

Response syntax:

Content-type: application/json

{
    "jobArn": "string",
    "jobId": "string",
    "description": "string"
Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobArn</td>
<td>JobArn</td>
<td>no</td>
<td>The job ARN.</td>
</tr>
<tr>
<td>jobId</td>
<td>JobId</td>
<td>no</td>
<td>The unique identifier you assigned to this job.</td>
</tr>
<tr>
<td>description</td>
<td>JobDescription</td>
<td>no</td>
<td>The job description.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException
- The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  - HTTP response code: 400

ResourceNotFoundException
- The specified resource does not exist.
  - HTTP response code: 404

ResourceAlreadyExistsException
- The resource already exists.
  - HTTP response code: 409

LimitExceededException
- A limit has been exceeded.
  - HTTP response code: 410

ThrottlingException
- The rate exceeds the limit.
  - HTTP response code: 429

ServiceUnavailableException
- The service is temporarily unavailable.
  - HTTP response code: 503

cli

Synopsis:

```
aws iot create-job \
  --job-id <value> \
  --targets <value> \
  [--document-source <value>] \
  [--document <value>] \
  [--description <value>] \
  [--presigned-url-config <value>] \
```
CreateJob

[--target-selection <value>] \
[--job-executions-rollout-config <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]

cli-input-json format:

```json
{
  "jobId": "string",
  "targets": [
    "string"
  ],
  "documentSource": "string",
  "document": "string",
  "description": "string",
  "presignedUrlConfig": {
    "roleArn": "string",
    "expiresInSec": "long"
  },
  "targetSelection": "string",
  "jobExecutionsRolloutConfig": {
    "maximumPerMinute": "integer"
  }
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>A job identifier which must be unique for your AWS account. We recommend using a UUID. Alpha-numeric characters, &quot;.&quot; and &quot;_&quot; are valid for use here.</td>
</tr>
<tr>
<td>targets</td>
<td>list</td>
<td>A list of things and thing groups to which the job should be sent.</td>
</tr>
<tr>
<td>documentSource</td>
<td>string</td>
<td>An S3 link to the job document.</td>
</tr>
<tr>
<td>document</td>
<td>string</td>
<td>The job document.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>A short text description of the job.</td>
</tr>
<tr>
<td>presignedUrlConfig</td>
<td>PresignedUrlConfig</td>
<td>Configuration information for pre-signed S3 URLs.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of an IAM role that grants permission to download files from the S3 bucket where the job data/updates are stored. The role</td>
</tr>
</tbody>
</table>
### CreateJob

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>expiresInSec</td>
<td>long</td>
<td>How long (in seconds) pre-signed URLs are valid. Valid values are 60 - 3600, the default value is 3600 seconds. Pre-signed URLs are generated when Jobs receives an MQTT request for the job document.</td>
</tr>
<tr>
<td>targetSelection</td>
<td>string</td>
<td>Specifies whether the job will continue to run (CONTINUOUS), or will be complete after all those things specified as targets have completed the job (SNAPSHOT). If continuous, the job may also be run on a thing when a change is detected in a target. For example, a job will run on a thing when the thing is added to a target group, even after the job was completed by all things originally in the group.</td>
</tr>
<tr>
<td>jobExecutionsRolloutConfig</td>
<td>JobExecutionsRolloutConfig</td>
<td>Allows you to create a staged rollout of the job.</td>
</tr>
<tr>
<td>maximumPerMinute</td>
<td>integer</td>
<td>The maximum number of things that will be notified of a pending job, per minute. This parameter allows you to create a staged rollout.</td>
</tr>
</tbody>
</table>

**Output:**

```json
{
  "jobArn": "string",
  "jobId": "string",
  "description": "string"
}
```

### cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobArn</td>
<td>string</td>
<td>The job ARN.</td>
</tr>
<tr>
<td>jobld</td>
<td>string</td>
<td>The unique identifier you assigned to this job.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobArn</td>
<td>string</td>
<td>The job ARN.</td>
</tr>
<tr>
<td>jobld</td>
<td>string</td>
<td>The unique identifier you assigned to this job.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobArn</td>
<td>string</td>
<td>The job ARN.</td>
</tr>
<tr>
<td>jobld</td>
<td>string</td>
<td>The unique identifier you assigned to this job.</td>
</tr>
</tbody>
</table>
Create Keys and Certificate

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>string</td>
<td>The job description.</td>
</tr>
<tr>
<td>length- max:2028</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pattern: [^\p{C}]+</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceNotFoundException

The specified resource does not exist.

ResourceAlreadyExistsException

The resource already exists.

LimitExceededException

A limit has been exceeded.

ThrottlingException

The rate exceeds the limit.

ServiceUnavailableException

The service is temporarily unavailable.

CreateKeysAndCertificate

Creates a 2048-bit RSA key pair and issues an X.509 certificate using the issued public key.

Note This is the only time AWS IoT issues the private key for this certificate, so it is important to keep it in a secure location.

https

Request syntax:

POST /keys-and-certificate?setAsActive=setAsActive

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>setAsActive</td>
<td>SetAsActive</td>
<td>no</td>
<td>Specifies whether the certificate is active.</td>
</tr>
</tbody>
</table>

Response syntax:
Content-type: application/json

{
  "certificateArn": "string",
  "certificateId": "string",
  "certificatePem": "string",
  "keyPair": {
    "PublicKey": "string",
    "PrivateKey": "string"
  }
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateArn</td>
<td>CertificateArn</td>
<td>no</td>
<td>The ARN of the certificate.</td>
</tr>
<tr>
<td>certificateId</td>
<td>CertificateId</td>
<td>no</td>
<td>The ID of the certificate. AWS IoT issues a default subject name for the certificate (for example, AWS IoT Certificate).</td>
</tr>
<tr>
<td>certificatePem</td>
<td>CertificatePem</td>
<td>no</td>
<td>The certificate data, in PEM format.</td>
</tr>
<tr>
<td>keyPair</td>
<td>KeyPair</td>
<td>no</td>
<td>The generated key pair.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUn bekommenException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500
**cli**

**Synopsis:**

```bash
aws iot create-keys-and-certificate \
   [--set-as-active | --no-set-as-active] \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
   "setAsActive": "boolean"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>setAsActive</td>
<td>boolean</td>
<td>Specifies whether the certificate is active.</td>
</tr>
</tbody>
</table>

**Output:**

```json
{
   "certificateArn": "string",
   "certificateId": "string",
   "certificatePem": "string",
   "keyPair": {
      "PublicKey": "string",
      "PrivateKey": "string"
   }
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateArn</td>
<td>string</td>
<td>The ARN of the certificate.</td>
</tr>
<tr>
<td>certificateId</td>
<td>string</td>
<td>The ID of the certificate. AWS IoT issues a default subject name for the certificate (for example, AWS IoT Certificate).</td>
</tr>
<tr>
<td>certificatePem</td>
<td>string</td>
<td>The certificate data, in PEM format.</td>
</tr>
<tr>
<td>keyPair</td>
<td>KeyPair</td>
<td>The generated key pair.</td>
</tr>
<tr>
<td>PublicKey</td>
<td>string</td>
<td>The public key.</td>
</tr>
<tr>
<td>PrivateKey</td>
<td>string</td>
<td>The private key.</td>
</tr>
</tbody>
</table>
Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

CreateOTAUpdate

Creates an AWS IoT OTAUpdate on a target group of things or groups.

https

Request syntax:

```json
POST /otaUpdates/otaUpdateId
Content-type: application/json

{
    "description": "string",
    "targets": [
        "string"
    ],
    "targetSelection": "string",
    "files": [
        {
            "fileName": "string",
            "fileVersion": "string",
            "fileSource": {
                "streamId": "string",
                "fileId": "integer"
            },
            "codeSigning": {
                "awsSignerJobId": "string",
                "customCodeSigning": {
                    "signature": {
                        "stream": {
                            "streamId": "string",
                            "fileId": "integer"
                        },
                        "inlineDocument": "blob"
                    },
                    "certificateChain": {
                        "stream": {
                            "streamId": "string"
                        }
                    }
                }
            }
        }
    ]
}
```
CreateOTAUpdate

```
{"fileId": "integer",
  "certificateName": "string",
  "inlineDocument": "string"
},
{"hashAlgorithm": "string",
  "signatureAlgorithm": "string"
},
{"attributes": {
  "string": "string"
}},
{"roleArn": "string",
  "additionalParameters": {
    "string": "string"
  }
}
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>otaUpdateId</td>
<td>OTAUpdateId</td>
<td>yes</td>
<td>The ID of the OTA update to be created.</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>OTAUpdateDescription</td>
<td>no</td>
<td>The description of the OTA update.</td>
</tr>
<tr>
<td>targets</td>
<td>Targets</td>
<td>yes</td>
<td>The targeted devices to receive OTA updates.</td>
</tr>
<tr>
<td>targetSelection</td>
<td>TargetSelection</td>
<td>no</td>
<td>Specifies whether the update will continue to run (CONTINUOUS), or will be complete after all the things specified as targets have completed the update (SNAPSHOT). If continuous, the update may also be run on a thing when a change is detected in a target. For example, an update will run on a thing when the thing is added to a target group, even after the update was completed by all things originally in the group. Valid values: CONTINUOUS</td>
</tr>
</tbody>
</table>
CreateOTAUpdate

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>files</td>
<td>OTAUpdateFiles</td>
<td>yes</td>
<td>The files to be streamed by the OTA update.</td>
</tr>
<tr>
<td>roleArn</td>
<td>RoleArn</td>
<td>yes</td>
<td>The IAM role that allows access to the AWS IoT Jobs service.</td>
</tr>
<tr>
<td>additionalParameters</td>
<td>AdditionalParameterMap</td>
<td>no</td>
<td>A list of additional OTA update parameters which are name-value pairs.</td>
</tr>
</tbody>
</table>

Response syntax:

```
Content-type: application/json
{
  "otaUpdateId": "string",
  "awsIotJobId": "string",
  "otaUpdateArn": "string",
  "awsIotJobArn": "string",
  "otaUpdateStatus": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>otaUpdateId</td>
<td>OTAUpdateId</td>
<td>no</td>
<td>The OTA update ID.</td>
</tr>
<tr>
<td>awsIotJobId</td>
<td>AwsIotJobId</td>
<td>no</td>
<td>The AWS IoT job ID associated with the OTA update.</td>
</tr>
<tr>
<td>otaUpdateArn</td>
<td>OTAUpdateArn</td>
<td>no</td>
<td>The OTA update ARN.</td>
</tr>
<tr>
<td>awsIotJobArn</td>
<td>AwsIotJobArn</td>
<td>no</td>
<td>The AWS IoT job ARN associated with the OTA update.</td>
</tr>
<tr>
<td>otaUpdateStatus</td>
<td>OTAUpdateStatus</td>
<td>no</td>
<td>The OTA update status.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.
HTTP response code: 404
ResourceAlreadyExistsException
   The resource already exists.
HTTP response code: 409
ThrottlingException
   The rate exceeds the limit.
HTTP response code: 429
UnauthorizedException
   You are not authorized to perform this operation.
HTTP response code: 401
InternalFailureException
   An unexpected error has occurred.
HTTP response code: 500
ServiceUnavailableException
   The service is temporarily unavailable.
HTTP response code: 503

cli

Synopsis:

```
aws iot create-ota-update \
   --ota-update-id <value> \
   [--description <value>] \n   [--targets <value>] \n   [--target-selection <value>] \n   --files <value> \n   --role-arn <value> \n   [--additional-parameters <value>] \n   [--cli-input-json <value>] \n   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "otaUpdateId": "string",
   "description": "string",
   "targets": [
      "string"
   ],
   "targetSelection": "string",
   "files": [
      {
         "fileName": "string",
         "fileVersion": "string",
         "fileSource": {
            "streamId": "string",
            "fileId": "integer"
         },
         "codeSigning": {
            "awsSignerJobId": "string",
```
"customCodeSigning": {
  "signature": {
    "stream": {
      "streamId": "string",
      "fileId": "integer"
    },
    "inlineDocument": "blob"
  },
  "certificateChain": {
    "stream": {
      "streamId": "string",
      "fileId": "integer"
    },
    "certificateName": "string",
    "inlineDocument": "string"
  },
  "hashAlgorithm": "string",
  "signatureAlgorithm": "string"
},
"attributes": {
  "string": "string"
},
"roleArn": "string",
"additionalParameters": {
  "string": "string"
}
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>otaUpdateId</td>
<td>string</td>
<td>The ID of the OTA update to be created.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>The description of the OTA update.</td>
</tr>
<tr>
<td></td>
<td>length- max:2028 pattern: [^\p{C}]+</td>
<td></td>
</tr>
<tr>
<td>targets</td>
<td>list</td>
<td>The targeted devices to receive OTA updates.</td>
</tr>
<tr>
<td></td>
<td>member: Target</td>
<td></td>
</tr>
<tr>
<td>targetSelection</td>
<td>string</td>
<td>Specifies whether the update will continue to run (CONTINUOUS), or will be complete after all the things specified as targets have completed the update (SNAPSHOT). If continuous, the update may also be run on a thing when a change is detected in a target. For example, an update will run on a thing</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td></td>
<td>when the thing is added to a target group, even after the update was completed by all things originally in the group. Valid values: CONTINUOUS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>files list member: OTAUpdateFile</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The files to be streamed by the OTA update.</td>
</tr>
<tr>
<td>fileName</td>
<td>string</td>
<td>The name of the file.</td>
</tr>
<tr>
<td>fileVersion</td>
<td>string</td>
<td>The file version.</td>
</tr>
<tr>
<td>fileSource</td>
<td>Stream</td>
<td>The source of the file.</td>
</tr>
<tr>
<td>streamId</td>
<td>string</td>
<td>The stream ID.</td>
</tr>
<tr>
<td>fileld</td>
<td>integer</td>
<td>The ID of a file associated with a stream.</td>
</tr>
<tr>
<td>awsSignerJobId</td>
<td>string</td>
<td>The ID of the AWSSignerJob which was created to sign the file.</td>
</tr>
<tr>
<td>signature</td>
<td>CodeSigningSignature</td>
<td>The signature for the file.</td>
</tr>
<tr>
<td>stream</td>
<td>Stream</td>
<td>A stream of the code signing signature.</td>
</tr>
<tr>
<td>streamId</td>
<td>string</td>
<td>The stream ID.</td>
</tr>
<tr>
<td>fileld</td>
<td>integer</td>
<td>The ID of a file associated with a stream.</td>
</tr>
<tr>
<td>inlineDocument</td>
<td>blob</td>
<td>A base64 encoded binary representation of the code signing signature.</td>
</tr>
</tbody>
</table>
CreateOTAUpdate

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateChain</td>
<td>CodeSigningCertificateChain</td>
<td>The certificate chain.</td>
</tr>
<tr>
<td>stream</td>
<td>Stream</td>
<td>A stream of the certificate chain files.</td>
</tr>
<tr>
<td>streamId</td>
<td>string</td>
<td>The stream ID.</td>
</tr>
<tr>
<td>fileId</td>
<td>integer</td>
<td>The ID of a file associated with a stream.</td>
</tr>
<tr>
<td>certificateName</td>
<td>string</td>
<td>The name of the certificate.</td>
</tr>
<tr>
<td>inlineDocument</td>
<td>string</td>
<td>A base64 encoded binary representation of the code signing certificate chain.</td>
</tr>
<tr>
<td>hashAlgorithm</td>
<td>string</td>
<td>The hash algorithm used to code sign the file.</td>
</tr>
<tr>
<td>signatureAlgorithm</td>
<td>string</td>
<td>The signature algorithm used to code sign the file.</td>
</tr>
<tr>
<td>attributes</td>
<td>map</td>
<td>A list of name/attribute pairs.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role that allows access to the AWS IoT Jobs service.</td>
</tr>
<tr>
<td>additionalParameters</td>
<td>map</td>
<td>A list of additional OTA update parameters which are name-value pairs.</td>
</tr>
</tbody>
</table>

Output:

```
{
    "otaUpdateId": "string",
    "awsIotJobId": "string",
    "otaUpdateArn": "string",
    "awsIotJobArn": "string",
    "otaUpdateStatus": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>otaUpdateId</td>
<td>string</td>
<td>The OTA update ID.</td>
</tr>
<tr>
<td></td>
<td>length-</td>
<td>max:128 min:1 pattern: [a-zA-Z0-9_.]+</td>
</tr>
</tbody>
</table>
CreatePolicy

Creates an AWS IoT policy.

The created policy is the default version for the policy. This operation creates a policy version with a version identifier of 1 and sets 1 as the policy's default version.

https

Request syntax:

```plaintext
POST /policies/policyName
Content-type: application/json
```


```json
{
   "policyDocument": "string"
}
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>yes</td>
<td>The policy name.</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyDocument</td>
<td>PolicyDocument</td>
<td>yes</td>
<td>The JSON document that describes the policy. policyDocument must have a minimum length of 1, with a maximum length of 2048, excluding whitespace.</td>
</tr>
</tbody>
</table>

**Response syntax:**

```json
Content-type: application/json
{
   "policyName": "string",
   "policyArn": "string",
   "policyDocument": "string",
   "policyVersionId": "string"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>no</td>
<td>The policy name.</td>
</tr>
<tr>
<td>policyArn</td>
<td>PolicyArn</td>
<td>no</td>
<td>The policy ARN.</td>
</tr>
<tr>
<td>policyDocument</td>
<td>PolicyDocument</td>
<td>no</td>
<td>The JSON document that describes the policy.</td>
</tr>
<tr>
<td>policyVersionId</td>
<td>PolicyVersionId</td>
<td>no</td>
<td>The policy version ID.</td>
</tr>
</tbody>
</table>

**Errors:**

**ResourceAlreadyExistsException**

The resource already exists.

HTTP response code: 409
MalformedPolicyException

The policy documentation is not valid.

HTTP response code: 400

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot create-policy
   --policy-name <value>
   --policy-document <value>
   [--cli-input-json <value>]
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "policyName": "string",
   "policyDocument": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
<tr>
<td></td>
<td>length-</td>
<td>max:128 min:1</td>
</tr>
<tr>
<td></td>
<td>pattern:</td>
<td>[w+=,.@-]+</td>
</tr>
</tbody>
</table>
CreatePolicy

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyDocument</td>
<td>string</td>
<td>The JSON document that describes the policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>policyDocument</strong> must have a minimum length of 1, with a maximum length of 2048, excluding whitespace.</td>
</tr>
</tbody>
</table>

Output:

```json
{
    "policyName": "string",
    "policyArn": "string",
    "policyDocument": "string",
    "policyVersionId": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>length- max:128 min:1 pattern: [w+=,.@-]+</td>
</tr>
<tr>
<td>policyArn</td>
<td>string</td>
<td>The policy ARN.</td>
</tr>
<tr>
<td>policyDocument</td>
<td>string</td>
<td>The JSON document that describes the policy.</td>
</tr>
<tr>
<td>policyVersionId</td>
<td>string</td>
<td>The policy version ID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pattern: [0-9]+</td>
</tr>
</tbody>
</table>

**Errors:**

ResourceAlreadyExistsException

The resource already exists.

MalformedPolicyException

The policy documentation is not valid.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.
ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

CreatePolicyVersion

Creates a new version of the specified AWS IoT policy. To update a policy, create a new policy version. A managed policy can have up to five versions. If the policy has five versions, you must use DeletePolicyVersion to delete an existing version before you create a new one.

Optionally, you can set the new version as the policy's default version. The default version is the operative version (that is, the version that is in effect for the certificates to which the policy is attached).

https

Request syntax:

```plaintext
POST /policies/policyName/version?setAsDefault=setAsDefault
Content-type: application/json

{
  "policyDocument": "string"
}
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>yes</td>
<td>The policy name.</td>
</tr>
<tr>
<td>setAsDefault</td>
<td>SetAsDefault</td>
<td>no</td>
<td>Specifies whether the policy version is set as the default. When this parameter is true, the new policy version becomes the operative version (that is, the version that is in effect for the certificates to which the policy is attached).</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
</table>
Response syntax:

```
Content-type: application/json
{
  "policyArn": "string",
  "policyDocument": "string",
  "policyVersionId": "string",
  "isDefaultVersion": "boolean"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyArn</td>
<td>PolicyArn</td>
<td>no</td>
<td>The policy ARN.</td>
</tr>
<tr>
<td>policyDocument</td>
<td>PolicyDocument</td>
<td>no</td>
<td>The JSON document that describes the policy.</td>
</tr>
<tr>
<td>policyVersionId</td>
<td>PolicyVersionId</td>
<td>no</td>
<td>The policy version ID.</td>
</tr>
<tr>
<td>isDefaultVersion</td>
<td>IsDefaultVersion</td>
<td>no</td>
<td>Specifies whether the policy version is the default.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

MalformedPolicyException

The policy documentation is not valid.

HTTP response code: 400

VersionsLimitExceededException

The number of policy versions exceeds the limit.

HTTP response code: 409

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429
UnauthorizedException
You are not authorized to perform this operation.
HTTP response code: 401

ServiceUnavailableException
The service is temporarily unavailable.
HTTP response code: 503

InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

cli

Synopsis:

```
aws iot create-policy-version \
  --policy-name <value> \
  --policy-document <value> \
  [--set-as-default | --no-set-as-default] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "policyName": "string",
  "policyDocument": "string",
  "setAsDefault": "boolean"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w+=,.@-]+</td>
<td></td>
</tr>
<tr>
<td>policyDocument</td>
<td>string</td>
<td>The JSON document that describes the policy. Minimum length of 1. Maximum length of 2048, excluding whitespace.</td>
</tr>
<tr>
<td>setAsDefault</td>
<td>boolean</td>
<td>Specifies whether the policy version is set as the default. When this parameter is true, the new policy version becomes the operative version (that is, the version that is in effect for the</td>
</tr>
</tbody>
</table>
Name | Type | Description
--- | --- | ---
| | | certificates to which the policy is attached).

Output:

```
{
    "policyArn": "string",
    "policyDocument": "string",
    "policyVersionId": "string",
    "isDefaultVersion": "boolean"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyArn</td>
<td>string</td>
<td>The policy ARN.</td>
</tr>
<tr>
<td>policyDocument</td>
<td>string</td>
<td>The JSON document that describes the policy.</td>
</tr>
<tr>
<td>policyVersionId</td>
<td>string</td>
<td>The policy version ID.</td>
</tr>
<tr>
<td>pattern: [0-9]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>isDefaultVersion</td>
<td>boolean</td>
<td>Specifies whether the policy version is the default.</td>
</tr>
</tbody>
</table>

Errors:

**ResourceNotFoundException**

The specified resource does not exist.

**MalformedPolicyException**

The policy documentation is not valid.

**VersionsLimitExceeded**

The number of policy versions exceeds the limit.

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

**ThrottlingException**

The rate exceeds the limit.

**UnauthorizedException**

You are not authorized to perform this operation.

**ServiceUnavailableException**

The service is temporarily unavailable.
InternalFailureException
An unexpected error has occurred.

CreateRoleAlias

Creates a role alias.

https

Request syntax:

POST /role-aliases/roleAlias
Content-type: application/json

{  
  "roleArn": "string",
  "credentialDurationSeconds": "integer"
}

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleAlias</td>
<td>RoleAlias</td>
<td>yes</td>
<td>The role alias that points to a role ARN. This allows you to change the role without having to update the device.</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>RoleArn</td>
<td>yes</td>
<td>The role ARN.</td>
</tr>
<tr>
<td>credentialDurationSeconds</td>
<td>CredentialDurationSeconds</td>
<td>no</td>
<td>How long (in seconds) the credentials will be valid.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{  
  "roleAlias": "string",
  "roleAliasArn": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleAlias</td>
<td>RoleAlias</td>
<td>no</td>
<td>The role alias.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Req?</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------</td>
<td>------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>roleAliasArn</td>
<td>RoleAliasArn</td>
<td>no</td>
<td>The role alias ARN.</td>
</tr>
</tbody>
</table>

**Errors:**

ResourceAlreadyExistsException

The resource already exists.

HTTP response code: 409

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

LimitExceededException

A limit has been exceeded.

HTTP response code: 410

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

**cli**

**Synopsis:**

```bash
aws iot create-role-alias \
  --role-alias <value> \
  --role-arn <value> \
  [--credential-duration-seconds <value>] \
  [--cli-input-json <value>]
```
CreateRoleAlias

cli-input-json format:

```json
{
   "roleAlias": "string",
   "roleArn": "string",
   "credentialDurationSeconds": "integer"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleAlias</td>
<td>string</td>
<td>The role alias that points to a role ARN. This allows you to change the role without having to update the device.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w=,@-]+</td>
<td></td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The role ARN.</td>
</tr>
<tr>
<td></td>
<td>length- max:2048 min:20</td>
<td></td>
</tr>
<tr>
<td>credentialDurationSeconds</td>
<td>integer</td>
<td>How long (in seconds) the credentials will be valid.</td>
</tr>
<tr>
<td></td>
<td>range- max:3600 min:900</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
   "roleAlias": "string",
   "roleAliasArn": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleAlias</td>
<td>string</td>
<td>The role alias.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w=,@-]+</td>
<td></td>
</tr>
<tr>
<td>roleAliasArn</td>
<td>string</td>
<td>The role alias ARN.</td>
</tr>
</tbody>
</table>

Errors:

ResourceAlreadyExistsException

The resource already exists.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
LimitExceededException

A limit has been exceeded.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

CreateScheduledAudit

Creates a scheduled audit that is run at a specified time interval.

**https**

**Request syntax:**

POST /audit/scheduledaudits/scheduledAuditName
Content-type: application/json

```json
{
    "frequency": "string",
    "dayOfMonth": "string",
    "dayOfWeek": "string",
    "targetCheckNames": [
        "string"
    ]
}
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditName</td>
<td>ScheduledAuditName</td>
<td>yes</td>
<td>The name you want to give to the scheduled audit. (Max. 128 chars)</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>AuditFrequency</td>
<td>yes</td>
<td>How often the scheduled audit takes place. Can be one of &quot;DAILY&quot;, &quot;WEEKLY&quot;,</td>
</tr>
</tbody>
</table>
### CreateScheduledAudit

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td></td>
<td></td>
<td>&quot;BIWEEKLY&quot; or &quot;MONTHLY&quot;. The actual start time of each audit is determined by the system.</td>
</tr>
<tr>
<td>dayOfMonth</td>
<td>DayOfMonth</td>
<td>no</td>
<td>The day of the month on which the scheduled audit takes place. Can be &quot;1&quot; through &quot;31&quot; or &quot;LAST&quot;. This field is required if the &quot;frequency&quot; parameter is set to &quot;MONTHLY&quot;. If days 29-31 are specified, and the month does not have that many days, the audit takes place on the &quot;LAST&quot; day of the month.</td>
</tr>
<tr>
<td>dayOfWeek</td>
<td>DayOfWeek</td>
<td>no</td>
<td>The day of the week on which the scheduled audit takes place. Can be one of &quot;SUN&quot;, &quot;MON&quot;, &quot;TUE&quot;, &quot;WED&quot;, &quot;THU&quot;, &quot;FRI&quot; or &quot;SAT&quot;. This field is required if the &quot;frequency&quot; parameter is set to &quot;WEEKLY&quot; or &quot;BIWEEKLY&quot;.</td>
</tr>
<tr>
<td>targetCheckNames</td>
<td>TargetAuditCheckNames</td>
<td>yes</td>
<td>Which checks are performed during the scheduled audit. Checks must be enabled for your account. (Use DescribeAccountAuditConfiguration to see the list of all checks including those that are enabled or UpdateAccountAuditConfiguration to select which checks are enabled.)</td>
</tr>
</tbody>
</table>

**Response syntax:**

```json
Content-type: application/json

{
  "scheduledAuditArn": "string"
}
```
Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditArn</td>
<td>ScheduledAuditArn</td>
<td>no</td>
<td>The ARN of the scheduled audit.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

LimitExceededException

A limit has been exceeded.

HTTP response code: 410

cli

Synopsis:

```
aws iot create-scheduled-audit \
  --frequency <value> \
  [--day-of-month <value>] \
  [--day-of-week <value>] \
  --target-check-names <value> \
  --scheduled-audit-name <value>  \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "frequency": "string",
  "dayOfMonth": "string",
  "dayOfWeek": "string",
  "targetCheckNames": ["string"],
  "scheduledAuditName": "string"
}
```
cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>string</td>
<td>How often the scheduled audit takes place. Can be one of &quot;DAILY&quot;, &quot;WEEKLY&quot;, &quot;BIWEEKLY&quot; or &quot;MONTHLY&quot;. The actual start time of each audit is determined by the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: DAILY</td>
</tr>
<tr>
<td>dayOfMonth</td>
<td>string</td>
<td>The day of the month on which the scheduled audit takes place. Can be &quot;1&quot; through &quot;31&quot; or &quot;LAST&quot;. This field is required if the &quot;frequency&quot; parameter is set to &quot;MONTHLY&quot;. If days 29-31 are specified, and the month does not have that many days, the audit takes place on the &quot;LAST&quot; day of the month.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pattern: ^([1-9]</td>
</tr>
<tr>
<td>dayOfWeek</td>
<td>string</td>
<td>The day of the week on which the scheduled audit takes place. Can be one of &quot;SUN&quot;, &quot;MON&quot;, &quot;TUE&quot;, &quot;WED&quot;, &quot;THU&quot;, &quot;FRI&quot; or &quot;SAT&quot;. This field is required if the &quot;frequency&quot; parameter is set to &quot;WEEKLY&quot; or &quot;BIWEEKLY&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: SUN</td>
</tr>
<tr>
<td>targetCheckNames</td>
<td>list</td>
<td>Which checks are performed during the scheduled audit. Checks must be enabled for your account. (Use DescribeAccountAuditConfiguration to see the list of all checks including those that are enabled or UpdateAccountAuditConfiguration to select which checks are enabled.)</td>
</tr>
<tr>
<td></td>
<td>member: AuditCheckName</td>
<td></td>
</tr>
<tr>
<td>scheduledAuditName</td>
<td>string</td>
<td>The name you want to give to the scheduled audit. (Max. 128 chars)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9_-]+</td>
</tr>
</tbody>
</table>

Output:

```
{
  "scheduledAuditArn": "string"
}
```
cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditArn</td>
<td>string</td>
<td>The ARN of the scheduled audit.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

LimitExceededError

A limit has been exceeded.

CreateSecurityProfile

Creates a Device Defender security profile.

https

Request syntax:

```
POST /security-profiles/securityProfileName
Content-type: application/json

{
    "securityProfileDescription": "string",
    "behaviors": [
        {
            "name": "string",
            "metric": "string",
            "criteria": {
                "comparisonOperator": "string",
                "value": {
                    "count": "long",
                    "cidrs": [
                        "string"
                    ],
                    "ports": [
                        "integer"
                    ]
                },
                "durationSeconds": "integer"
            }
        }
    ],
    "alertTargets": {
        "string": {
            "string": {
            }
        }
    }
}
```
"alertTargetArn": "string",
"roleArn": "string"
}
}

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>yes</td>
<td>The name you are giving to the security profile.</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileDescription</td>
<td>SecurityProfileDescription</td>
<td>no</td>
<td>A description of the security profile.</td>
</tr>
<tr>
<td>behaviors</td>
<td>Behaviors</td>
<td>yes</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td>alertTargets</td>
<td>AlertTargets</td>
<td>no</td>
<td>Specifies the destinations to which alerts are sent. (Alerts are always sent to the console.) Alerts are generated when a device (thing) violates a behavior.</td>
</tr>
</tbody>
</table>

**Response syntax:**

```
Content-type: application/json

{
  "securityProfileName": "string",
  "securityProfileArn": "string"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>no</td>
<td>The name you gave to the security profile.</td>
</tr>
<tr>
<td>securityProfileArn</td>
<td>SecurityProfileArn</td>
<td>no</td>
<td>The ARN of the security profile.</td>
</tr>
</tbody>
</table>

**Errors:**
**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ResourceAlreadyExistsException**

The resource already exists.

HTTP response code: 409

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

---

**cli**

**Synopsis:**

```
aws iot create-security-profile \
  --security-profile-name <value> \
  [--security-profile-description <value>] \
  --behaviors <value> \
  [--alert-targets <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

**cli-input-json format:**

```
{
  "securityProfileName": "string",
  "securityProfileDescription": "string",
  "behaviors": [
    {
      "name": "string",
      "metric": "string",
      "criteria": {
        "comparisonOperator": "string",
        "value": {
          "count": "long",
          "cidrs": [
            "string"
          ],
          "ports": [
            "integer"
          ],
          "durationSeconds": "integer"
        }
      },
      "alertTargets": {
      }
    }
  ]
}
```
cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name you are giving to the security profile.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>securityProfileDescription</td>
<td>string</td>
<td>A description of the security profile.</td>
</tr>
<tr>
<td></td>
<td>length- max:1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [\p{Graph}]*</td>
<td></td>
</tr>
<tr>
<td>behaviors</td>
<td>list member: Behavior</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the behavior.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>metric</td>
<td>string</td>
<td>What is measured by the behavior.</td>
</tr>
<tr>
<td>criteria</td>
<td>BehaviorCriteria</td>
<td>The criteria that determine if a device is behaving normally in regard to the metric.</td>
</tr>
<tr>
<td>comparisonOperator</td>
<td>string</td>
<td>The operator that relates the thing measured (metric) to the criteria (value).</td>
</tr>
<tr>
<td></td>
<td>enum: less-than</td>
<td></td>
</tr>
<tr>
<td></td>
<td>less-than-equals</td>
<td></td>
</tr>
<tr>
<td></td>
<td>greater-than</td>
<td></td>
</tr>
<tr>
<td></td>
<td>greater-than-equals</td>
<td></td>
</tr>
<tr>
<td></td>
<td>in-cidr-set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>not-in-cidr-set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>in-port-set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>not-in-port-set</td>
<td></td>
</tr>
<tr>
<td>value</td>
<td>MetricValue</td>
<td>The value to be compared with the metric.</td>
</tr>
<tr>
<td>count</td>
<td>long</td>
<td>If the comparisonOperator calls for a numeric value, use this to specify that numeric value to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>range- min:0</td>
<td></td>
</tr>
<tr>
<td>cidrs</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of CIDRs, use</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>member: Cidr</td>
<td>list</td>
<td>this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>member: Port</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of ports, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>durationSeconds</td>
<td>integer</td>
<td>Use this to specify the period of time over which the behavior is evaluated, for those criteria which have a time dimension (for example, NUM_MESSAGES_SENT).</td>
</tr>
<tr>
<td>alertTargets</td>
<td>map</td>
<td>Specifies the destinations to which alerts are sent. (Alerts are always sent to the console.) Alerts are generated when a device (thing) violates a behavior.</td>
</tr>
<tr>
<td>alertTargetArn</td>
<td>string</td>
<td>The ARN of the notification target to which alerts are sent.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants permission to send alerts to the notification target.</td>
</tr>
</tbody>
</table>

Output:

```
{
  "securityProfileName": "string",
  "securityProfileArn": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name you gave to the security profile.</td>
</tr>
<tr>
<td>securityProfileArn</td>
<td>string</td>
<td>The ARN of the security profile.</td>
</tr>
</tbody>
</table>

**Errors:**

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
CreateStream

Creates a stream for delivering one or more large files in chunks over MQTT. A stream transports data bytes in chunks or blocks packaged as MQTT messages from a source like S3. You can have one or more files associated with a stream. The total size of a file associated with the stream cannot exceed more than 2 MB. The stream will be created with version 0. If a stream is created with the same streamID as a stream that existed and was deleted within last 90 days, we will resurrect that old stream by incrementing the version by 1.

https

Request syntax:

POST /streams/streamId
Content-type: application/json

{  
  "description": "string",
  "files": [
    {
      "fileId": "integer",
      "s3Location": {
        "bucket": "string",
        "key": "string",
        "version": "string"
      }
    }
  ],
  "roleArn": "string"
}

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streamId</td>
<td>StreamId</td>
<td>yes</td>
<td>The stream ID.</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>StreamDescription</td>
<td>no</td>
<td>A description of the stream.</td>
</tr>
<tr>
<td>files</td>
<td>StreamFiles</td>
<td>yes</td>
<td>The files to stream.</td>
</tr>
</tbody>
</table>
CreateStream

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>RoleArn</td>
<td>yes</td>
<td>An IAM role that allows the IoT service principal assumes to access your S3 files.</td>
</tr>
</tbody>
</table>

**Response syntax:**

Content-type: application/json

```json
{
  "streamId": "string",
  "streamArn": "string",
  "description": "string",
  "streamVersion": "integer"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streamId</td>
<td>StreamId</td>
<td>no</td>
<td>The stream ID.</td>
</tr>
<tr>
<td>streamArn</td>
<td>StreamArn</td>
<td>no</td>
<td>The stream ARN.</td>
</tr>
<tr>
<td>description</td>
<td>StreamDescription</td>
<td>no</td>
<td>A description of the stream.</td>
</tr>
<tr>
<td>streamVersion</td>
<td>StreamVersion</td>
<td>no</td>
<td>The version of the stream.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404

**ResourceAlreadyExistsException**

The resource already exists.

HTTP response code: 409

**ThrottlingException**

The rate exceeds the limit.
HTTP response code: 429
UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401
ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503
InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

aws iot create-stream \
    --stream-id <value> \
    [--description <value>] \
    --files <value> \
    --role-arn <value> \n    [--cli-input-json <value>] \n    [--generate-cli-skeleton]

cli-input-json format:

{  
    "streamId": "string",  
    "description": "string",  
    "files": [  
        {  
            "fileId": "integer",  
            "s3Location": {  
                "bucket": "string",  
                "key": "string",  
                "version": "string"  
            }  
        }]  
    }  
    "roleArn": "string"  
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streamId</td>
<td>string</td>
<td>The stream ID.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9_-]+</td>
<td></td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>A description of the stream.</td>
</tr>
</tbody>
</table>
AWS IoT Developer Guide
CreateStream

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>files</td>
<td>list</td>
<td>The files to stream.</td>
</tr>
<tr>
<td>member:</td>
<td>StreamFile</td>
<td></td>
</tr>
<tr>
<td>fileId</td>
<td>integer</td>
<td>The file ID.</td>
</tr>
<tr>
<td>range-</td>
<td>max:255</td>
<td>min:0</td>
</tr>
<tr>
<td>s3Location</td>
<td>S3Location</td>
<td>The location of the file in S3.</td>
</tr>
<tr>
<td>bucket</td>
<td>string</td>
<td>The S3 bucket that contains the file to stream.</td>
</tr>
<tr>
<td>key</td>
<td>string</td>
<td>The name of the file within the S3 bucket to stream.</td>
</tr>
<tr>
<td>version</td>
<td>string</td>
<td>The file version.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>An IAM role that allows the IoT service principal assumes to access your S3 files.</td>
</tr>
<tr>
<td>length-</td>
<td>max:2028</td>
<td>pattern: [^\p{C}]+</td>
</tr>
<tr>
<td>length-</td>
<td>min:1</td>
<td>-pattern: [a-zA-Z0-9-_.]+</td>
</tr>
<tr>
<td>length-</td>
<td>max:2048 min:0</td>
<td>-pattern: [^\p{C}]+</td>
</tr>
</tbody>
</table>

Output:

```json
{
    "streamId": "string",
    "streamArn": "string",
    "description": "string",
    "streamVersion": "integer"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streamId</td>
<td>string</td>
<td>The stream ID.</td>
</tr>
<tr>
<td>length-</td>
<td>max:128 min:1</td>
<td>pattern: [a-zA-Z0-9-_.]+</td>
</tr>
<tr>
<td>streamArn</td>
<td>string</td>
<td>The stream ARN.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>A description of the stream.</td>
</tr>
<tr>
<td>length-</td>
<td>max:2028</td>
<td>pattern: [^\p{C}]+</td>
</tr>
<tr>
<td>streamVersion</td>
<td>integer</td>
<td>The version of the stream.</td>
</tr>
<tr>
<td>range-</td>
<td>max:65535 min:0</td>
<td></td>
</tr>
</tbody>
</table>
Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceNotFoundException

The specified resource does not exist.

ResourceAlreadyExistsException

The resource already exists.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

CreateThing

Creates a thing record in the registry.

Note

This is a control plane operation. See Authorization for information about authorizing control plane actions.

https

Request syntax:

```
POST /things/thingName
Content-type: application/json

{
  "thingTypeName": "string",
  "attributePayload": {
    "attributes": {
      "string": "string"
    },
    "merge": "boolean"
  }
}
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing to create.</td>
</tr>
</tbody>
</table>
Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>ThingTypeName</td>
<td>no</td>
<td>The name of the thing type associated with the new thing.</td>
</tr>
</tbody>
</table>
| attributePayload | AttributePayload | no   | The attribute payload, which consists of up to three name/value pairs in a JSON document. For example: 
  
  \"attributes\": 
  \{ 
  \"string1\": 
  \"string2\" 
  \} |

Response syntax:

```json
Content-type: application/json
{
  "thingName": "string",
  "thingArn": "string",
  "thingId": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>no</td>
<td>The name of the new thing.</td>
</tr>
<tr>
<td>thingArn</td>
<td>ThingArn</td>
<td>no</td>
<td>The ARN of the new thing.</td>
</tr>
<tr>
<td>thingId</td>
<td>ThingId</td>
<td>no</td>
<td>The thing ID.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.
HTTP response code: 401
ServiceUnavailableException
The service is temporarily unavailable.

HTTP response code: 503
InternalFailureException
An unexpected error has occurred.

HTTP response code: 500
ResourceAlreadyExistsException
The resource already exists.

HTTP response code: 409
ResourceNotFoundException
The specified resource does not exist.

HTTP response code: 404

cli

Synopsis:

aws iot create-thing \
  --thing-name <value> \
  [--thing-type-name <value>] \
  [--attribute-payload <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]

cli-input-json format:

{
  "thingName": "string",
  "thingTypeName": "string",
  "attributePayload": {
    "attributes": {
      "string": "string"
    },
    "merge": "boolean"
  }
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing to create.</td>
</tr>
<tr>
<td></td>
<td>length: max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9_:-.]+</td>
<td></td>
</tr>
</tbody>
</table>
CreateThing

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>string</td>
<td>The name of the thing type associated with the new thing.</td>
</tr>
<tr>
<td>length- max:128 min:1</td>
<td>pattern: [a-zA-Z0-9_:-]+</td>
<td></td>
</tr>
<tr>
<td>attributePayload</td>
<td>AttributePayload</td>
<td>The attribute payload, which consists of up to three name/value pairs in a JSON document. For example:</td>
</tr>
<tr>
<td>attributes</td>
<td>map</td>
<td>A JSON string containing up to three key-value pairs in JSON format. For example:</td>
</tr>
<tr>
<td>merge</td>
<td>boolean</td>
<td>Specifies whether the list of attributes provided in the AttributePayload is merged with the attributes stored in the registry, instead of overwriting them. To remove an attribute, call UpdateThing with an empty attribute value.</td>
</tr>
</tbody>
</table>

**Note**
The merge attribute is only valid when calling UpdateThing.

Output:

```json
{
  "thingName": "string",
  "thingArn": "string",
  "thingId": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the new thing.</td>
</tr>
<tr>
<td>length-</td>
<td>max:128</td>
<td></td>
</tr>
<tr>
<td>min:1</td>
<td>pattern: [a-zA-Z0-9_:-]+</td>
<td></td>
</tr>
</tbody>
</table>
CreateThingGroup

Create a thing group.

**Note**
This is a control plane operation. See Authorization for information about authorizing control plane actions.

**https**

**Request syntax:**

```json
POST /thing-groups/thingGroupName
Content-type: application/json

{
    "parentGroupName": "string",
    "thingGroupProperties": {
        "thingGroupDescription": "string",
        "attributePayload": {
            "attributes": {
                "string": "string"
            },
            "merge": "boolean"
        }
    }
}
```
**CreateThingGroup**

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>ThingGroupName</td>
<td>yes</td>
<td>The thing group name to create.</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>parentGroupName</td>
<td>ThingGroupName</td>
<td>no</td>
<td>The name of the parent thing group.</td>
</tr>
<tr>
<td>thingGroupProperties</td>
<td>ThingGroupProperties</td>
<td>no</td>
<td>The thing group properties.</td>
</tr>
</tbody>
</table>

**Response syntax:**

```
Content-type: application/json
{
  "thingGroupName": "string",
  "thingGroupArn": "string",
  "thingGroupId": "string"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>ThingGroupName</td>
<td>no</td>
<td>The thing group name.</td>
</tr>
<tr>
<td>thingGroupArn</td>
<td>ThingGroupArn</td>
<td>no</td>
<td>The thing group ARN.</td>
</tr>
<tr>
<td>thingGroupId</td>
<td>ThingGroupId</td>
<td>no</td>
<td>The thing group ID.</td>
</tr>
</tbody>
</table>

**Errors:**

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  
  HTTP response code: 400

- **ResourceAlreadyExistsException**
  
  The resource already exists.
  
  HTTP response code: 409
ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```bash
aws iot create-thing-group \
  --thing-group-name <value> \
  [--parent-group-name <value>] \
  [--thing-group-properties <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "thingGroupName": "string",
  "parentGroupName": "string",
  "thingGroupProperties": {
    "thingGroupDescription": "string",
    "attributePayload": {
      "attributes": {
        "string": "string"
      },
      "merge": "boolean"
    }
  }
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>string</td>
<td>The thing group name to create.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>parentGroupName</td>
<td>string</td>
<td>The name of the parent thing group.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>thingGroupProperties</td>
<td>ThingGroupProperties</td>
<td>The thing group properties.</td>
</tr>
<tr>
<td>thingGroupDescription</td>
<td>string</td>
<td>The thing group description.</td>
</tr>
<tr>
<td></td>
<td>length- max:2028</td>
<td></td>
</tr>
</tbody>
</table>
CreateThingGroup

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attributePayload</td>
<td>AttributePayload</td>
<td>The thing group attributes in JSON format.</td>
</tr>
<tr>
<td>attributes</td>
<td>map</td>
<td>A JSON string containing up to three key-value pair in JSON format. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;attributes&quot;: {&quot;string1&quot;: &quot;string2&quot;}</td>
</tr>
<tr>
<td>merge</td>
<td>boolean</td>
<td>Specifies whether the list of attributes provided in the AttributePayload is merged with the attributes stored in the registry, instead of overwriting them.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To remove an attribute, call UpdateThing with an empty attribute value.</td>
</tr>
</tbody>
</table>
|                           |                           | **Note**
|                           |                           | The `merge` attribute is only valid when calling UpdateThing.               |

Output:

```json
{
  "thingGroupName": "string",
  "thingGroupArn": "string",
  "thingGroupId": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>string</td>
<td>The thing group name.</td>
</tr>
<tr>
<td>thingGroupArn</td>
<td>string</td>
<td>The thing group ARN.</td>
</tr>
<tr>
<td>thingGroupId</td>
<td>string</td>
<td>The thing group ID.</td>
</tr>
</tbody>
</table>

Errors:
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceAlreadyExistsException

The resource already exists.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

CreateThingType

Creates a new thing type.

https

Request syntax:

POST /thing-types/thingTypeName
Content-type: application/json

{  
  "thingTypeProperties": {  
    "thingTypeDescription": "string",  
    "searchableAttributes": [  
      "string"  
    ]  
  }  
}

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>ThingTypeName</td>
<td>yes</td>
<td>The name of the thing type.</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeProperties</td>
<td>ThingTypeProperties</td>
<td>no</td>
<td>The ThingTypeProperties for the thing type to create. It contains information about the new thing type including a description, and a list of searchable thing attribute names.</td>
</tr>
</tbody>
</table>
Response syntax:

```
Content-type: application/json

{
    "thingTypeName": "string",
    "thingTypeArn": "string",
    "thingTypeId": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>ThingTypeName</td>
<td>no</td>
<td>The name of the thing type.</td>
</tr>
<tr>
<td>thingTypeArn</td>
<td>ThingTypeArn</td>
<td>no</td>
<td>The Amazon Resource Name (ARN) of the thing type.</td>
</tr>
<tr>
<td>thingTypeId</td>
<td>ThingTypeId</td>
<td>no</td>
<td>The thing type ID.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

ResourceAlreadyExistsException

The resource already exists.

HTTP response code: 409
cli

Synopsis:

```bash
aws iot create-thing-type \
  --thing-type-name <value> \ 
  [--thing-type-properties <value>] \ 
  [--cli-input-json <value>] \ 
  [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "thingTypeName": "string",
  "thingTypeProperties": {
    "thingTypeDescription": "string",
    "searchableAttributes": [
      "string"
    ]
  }
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>string</td>
<td>The name of the thing type.</td>
</tr>
<tr>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>thingTypeProperties</td>
<td>ThingTypeProperties</td>
<td>The ThingTypeProperties for the thing type to create. It contains information about the new thing type including a description, and a list of searchable thing attribute names.</td>
</tr>
<tr>
<td>thingTypeDescription</td>
<td>string</td>
<td>The description of the thing type.</td>
</tr>
<tr>
<td>length- max:2028 pattern: [\p{Graph}]*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>searchableAttributes</td>
<td>list</td>
<td>A list of searchable thing attribute names.</td>
</tr>
<tr>
<td>member: AttributeName java class: java.util.List</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
  "thingTypeName": "string",
  "thingTypeArn": "string",
  "thingTypeId": "string"
}
```
cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>string</td>
<td>The name of the thing type.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9;_-]+</td>
<td></td>
</tr>
<tr>
<td>thingTypeArn</td>
<td>string</td>
<td>The Amazon Resource Name (ARN) of the thing type.</td>
</tr>
<tr>
<td>thingTypeId</td>
<td>string</td>
<td>The thing type ID.</td>
</tr>
</tbody>
</table>

Errors:

- **InvalidRequestException**
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
- **ThrottlingException**
  - The rate exceeds the limit.
- **UnauthorizedException**
  - You are not authorized to perform this operation.
- **ServiceUnavailableException**
  - The service is temporarily unavailable.
- **InternalFailureException**
  - An unexpected error has occurred.
- **ResourceAlreadyExistsException**
  - The resource already exists.

CreateTopicRule

Creates a rule. Creating rules is an administrator-level action. Any user who has permission to create rules will be able to access data processed by the rule.

https

Request syntax:

```json
POST /rules/ruleName
Content-type: application/json
{
  "topicRulePayload": {
    "sql": "string",
    "description": "string",
    "actions": [
      "dynamoDB": {
```

666
"tableName": "string",
"roleArn": "string",
"operation": "string",
"hashKeyField": "string",
"hashKeyValue": "string",
"hashKeyType": "string",
"rangeKeyField": "string",
"rangeKeyValue": "string",
"rangeKeyType": "string",
"payloadField": "string"
},
"dynamoDBv2": { 
  "roleArn": "string",
  "putItem": { 
    "tableName": "string"
  }
},
"lambda": { 
  "functionArn": "string"
},
"sns": { 
  "targetArn": "string",
  "roleArn": "string",
  "messageFormat": "string"
},
"sqs": { 
  "roleArn": "string",
  "queueUrl": "string",
  "useBase64": "boolean"
},
"kinesis": { 
  "roleArn": "string",
  "streamName": "string",
  "partitionKey": "string"
},
"republish": { 
  "roleArn": "string",
  "topic": "string"
},
"s3": { 
  "roleArn": "string",
  "bucketName": "string",
  "key": "string",
  "cannedAcl": "string"
},
"firehose": { 
  "roleArn": "string",
  "deliveryStreamName": "string",
  "separator": "string"
},
"cloudwatchMetric": { 
  "roleArn": "string",
  "metricNamespace": "string",
  "metricName": "string",
  "metricValue": "string",
  "metricUnit": "string",
  "metricTimestamp": "string"
},
"cloudwatchAlarm": { 
  "roleArn": "string",
  "alarmName": "string",
  "stateReason": "string",
  "stateValue": "string"
},
"elasticsearch": { 
  "roleArn": "string",
  "endpoint": "string"
},

667
"endpoint": "string",
"index": "string",
"type": "string",
"id": "string"
},
"salesforce": {
  "token": "string",
  "url": "string"
},
"iotAnalytics": {
  "channelArn": "string",
  "channelName": "string",
  "roleArn": "string"
},
"stepFunctions": {
  "executionNamePrefix": "string",
  "stateMachineName": "string",
  "roleArn": "string"
}

"ruleDisabled": "boolean",
"awsIotSqlVersion": "string",
"errorAction": {
  "dynamoDB": {
    "tableName": "string",
    "roleArn": "string",
    "operation": "string",
    "hashKeyField": "string",
    "hashKeyValue": "string",
    "hashKeyType": "string",
    "rangeKeyField": "string",
    "rangeKeyValue": "string",
    "rangeKeyType": "string",
    "payloadField": "string"
  },
  "dynamoDBv2": {
    "roleArn": "string",
    "putItem": {
      "tableName": "string"
    }
  },
  "lambda": {
    "functionArn": "string"
  },
  "sns": {
    "targetArn": "string",
    "roleArn": "string",
    "messageFormat": "string"
  },
  "sqs": {
    "roleArn": "string",
    "queueUrl": "string",
    "useBase64": "boolean"
  },
  "kinesis": {
    "roleArn": "string",
    "streamName": "string",
    "partitionKey": "string"
  },
  "republish": {
    "roleArn": "string",
    "topic": "string"
  },
  "s3": {
    "roleArn": "string",
...
```
"bucketName": "string",
"key": "string",
"cannedAcl": "string"
},
"firehose": {
"roleArn": "string",
"deliveryStreamName": "string",
"separator": "string"
},
"cloudwatchMetric": {
"roleArn": "string",
"metricNamespace": "string",
"metricName": "string",
"metricValue": "string",
"metricUnit": "string",
"metricTimestamp": "string"
},
"cloudwatchAlarm": {
"roleArn": "string",
"alarmName": "string",
"stateReason": "string",
"stateValue": "string"
},
"elasticsearch": {
"roleArn": "string",
"endpoint": "string",
"index": "string",
"type": "string",
"id": "string"
},
"salesforce": {
"token": "string",
"url": "string"
},
"iotAnalytics": {
"channelArn": "string",
"channelName": "string",
"roleArn": "string"
},
"stepFunctions": {
"executionNamePrefix": "string",
"stateMachineName": "string",
"roleArn": "string"
}
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleName</td>
<td>RuleName</td>
<td>yes</td>
<td>The name of the rule.</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>topicRulePayload</td>
<td>TopicRulePayload</td>
<td>yes</td>
<td>The rule payload.</td>
</tr>
</tbody>
</table>

**Errors:**

669
SqlParseException
The Rule-SQL expression can't be parsed correctly.
HTTP response code: 400

InternalException
An unexpected error has occurred.
HTTP response code: 500

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an
UpdateJobExecution request contains invalid status details. The message contains details about the
error.
HTTP response code: 400

ResourceAlreadyExistsException
The resource already exists.
HTTP response code: 409

ServiceUnavailableException
The service is temporarily unavailable.
HTTP response code: 503

cli

Synopsis:

```bash
aws iot create-topic-rule \\
--rule-name <value> \\
--topic-rule-payload <value> \\
[--cli-input-json <value>] \\
[--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "ruleName": "string",
  "topicRulePayload": {
    "sql": "string",
    "description": "string",
    "actions": [
      {
        "dynamoDB": {
          "tableName": "string",
          "roleArn": "string",
          "operation": "string",
          "hashKeyField": "string",
          "hashKeyValue": "string",
          "hashKeyType": "string",
          "rangeKeyField": "string",
          "rangeKeyValue": "string",
          "rangeKeyType": "string",
          "payloadField": "string"
        },
        "dynamoDBv2": {
          "roleArn": "string",
```
"putItem": {
  "tableName": "string"
},
"lambda": {
  "functionArn": "string"
},
"sns": {
  "targetArn": "string",
  "roleArn": "string",
  "messageFormat": "string"
},
"sqs": {
  "roleArn": "string",
  "queueUrl": "string",
  "useBase64": "boolean"
},
"kinesis": {
  "roleArn": "string",
  "streamName": "string",
  "partitionKey": "string"
},
"republish": {
  "roleArn": "string",
  "topic": "string"
},
"s3": {
  "roleArn": "string",
  "bucketName": "string",
  "key": "string",
  "cannedAcl": "string"
},
"firehose": {
  "roleArn": "string",
  "deliveryStreamName": "string",
  "separator": "string"
},
"cloudwatchMetric": {
  "roleArn": "string",
  "metricNamespace": "string",
  "metricName": "string",
  "metricValue": "string",
  "metricUnit": "string",
  "metricTimestamp": "string"
},
"cloudwatchAlarm": {
  "roleArn": "string",
  "alarmName": "string",
  "stateReason": "string",
  "stateValue": "string"
},
"elasticsearch": {
  "roleArn": "string",
  "endpoint": "string",
  "index": "string",
  "type": "string",
  "id": "string"
},
"salesforce": {
  "token": "string",
  "url": "string"
},
"iotAnalytics": {
  "channelArn": "string",
  "channelName": "string",
  "roleArn": "string"
},
  "stepFunctions": {
    "executionNamePrefix": "string",
    "stateMachineName": "string",
    "roleArn": "string"
  }
},
"ruleDisabled": "boolean",
"awsIoTSqlVersion": "string",
"errorAction": {
  "dynamoDB": {
    "tableName": "string",
    "roleArn": "string",
    "operation": "string",
    "hashKeyField": "string",
    "hashKeyValue": "string",
    "hashKeyType": "string",
    "rangeKeyField": "string",
    "rangeKeyValue": "string",
    "rangeKeyType": "string",
    "payloadField": "string"
  },
  "dynamoDBv2": {
    "roleArn": "string",
    "putItem": {
      "tableName": "string"
    }
  },
  "lambda": {
    "functionArn": "string"
  },
  "sns": {
    "targetArn": "string",
    "roleArn": "string",
    "messageFormat": "string"
  },
  "sqs": {
    "roleArn": "string",
    "queueUrl": "string",
    "useBase64": "boolean"
  },
  "kinesis": {
    "roleArn": "string",
    "streamName": "string",
    "partitionKey": "string"
  },
  "republish": {
    "roleArn": "string",
    "topic": "string"
  },
  "s3": {
    "roleArn": "string",
    "bucketName": "string",
    "key": "string",
    "cannedAcl": "string"
  },
  "firehose": {
    "roleArn": "string",
    "deliveryStreamName": "string",
    "separator": "string"
  },
  "cloudwatchMetric": {
    "roleArn": "string",
    "metricNamespace": "string",
    "metricName": "string"}
cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleName</td>
<td>string</td>
<td>The name of the rule.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td>pattern: ^[a-zA-Z0-9_]+$</td>
</tr>
<tr>
<td>topicRulePayload</td>
<td>TopicRulePayload</td>
<td>The rule payload.</td>
</tr>
<tr>
<td>sql</td>
<td>string</td>
<td>The SQL statement used to query the topic. For more information, see <a href="https://aws.amazon.com">AWS IoT SQL Reference</a> in the <a href="https://aws.amazon.com">AWS IoT Developer Guide</a>.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>The description of the rule.</td>
</tr>
<tr>
<td>actions</td>
<td>list</td>
<td>The actions associated with the rule.</td>
</tr>
<tr>
<td></td>
<td>member: Action</td>
<td></td>
</tr>
<tr>
<td>dynamoDB</td>
<td>DynamoDBAction</td>
<td>Write to a DynamoDB table.</td>
</tr>
<tr>
<td>tableName</td>
<td>string</td>
<td>The name of the DynamoDB table.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the DynamoDB table.</td>
</tr>
<tr>
<td>operation</td>
<td>string</td>
<td>The type of operation to be performed. This follows the substitution template, so it can be <code>${operation}</code>, but the substitution must result in one of the following: INSERT, UPDATE, or DELETE.</td>
</tr>
<tr>
<td>hashKeyField</td>
<td>string</td>
<td>The hash key name.</td>
</tr>
<tr>
<td>hashKeyValue</td>
<td>string</td>
<td>The hash key value.</td>
</tr>
<tr>
<td>hashKeyType</td>
<td>string</td>
<td>The hash key type. Valid values are &quot;STRING&quot; or &quot;NUMBER&quot;.</td>
</tr>
<tr>
<td>rangeKeyField</td>
<td>string</td>
<td>The range key name.</td>
</tr>
<tr>
<td>rangeKeyValue</td>
<td>string</td>
<td>The range key value.</td>
</tr>
<tr>
<td>rangeKeyType</td>
<td>string</td>
<td>The range key type. Valid values are &quot;STRING&quot; or &quot;NUMBER&quot;.</td>
</tr>
<tr>
<td>payloadField</td>
<td>string</td>
<td>The action payload. This name can be customized.</td>
</tr>
<tr>
<td>dynamoDBv2</td>
<td>DynamoDBv2Action</td>
<td>Write to a DynamoDB table. This is a new version of the DynamoDB action. It allows you to write each attribute in an MQTT message payload into a separate DynamoDB column.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the DynamoDB table.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>putItem</td>
<td>PutItemInput</td>
<td>Specifies the DynamoDB table to which the message data will be written. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{ &quot;dynamoDBv2&quot;: { &quot;roleArn&quot;: &quot;aws:iam:12341251:my-role&quot; &quot;putItem&quot;: { &quot;tableName&quot;: &quot;my-table&quot; } } }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Each attribute in the message payload will be written to a separate column in the DynamoDB database.</td>
</tr>
<tr>
<td>tableName</td>
<td>string</td>
<td>The table where the message data will be written</td>
</tr>
<tr>
<td>lambda</td>
<td>LambdaAction</td>
<td>Invoke a Lambda function.</td>
</tr>
<tr>
<td>functionArn</td>
<td>string</td>
<td>The ARN of the Lambda function.</td>
</tr>
<tr>
<td>sns</td>
<td>SnsAction</td>
<td>Publish to an Amazon SNS topic.</td>
</tr>
<tr>
<td>targetArn</td>
<td>string</td>
<td>The ARN of the SNS topic.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>messageFormat</td>
<td>string</td>
<td>(Optional) The message format of the message to publish. Accepted values are &quot;JSON&quot; and &quot;RAW&quot;. The default value of the attribute is &quot;RAW&quot;. SNS uses this setting to determine if the payload should be parsed and relevant platform-specific bits of the payload should be extracted. To read more about SNS message formats, see <a href="http://docs.aws.amazon.com/sns/latest/dg/json-formats.html">http://docs.aws.amazon.com/sns/latest/dg/json-formats.html</a> refer to their official documentation.</td>
</tr>
<tr>
<td>sqs</td>
<td>SqsAction</td>
<td>Publish to an Amazon SQS queue.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>queueUrl</td>
<td>string</td>
<td>The URL of the Amazon SQS queue.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>useBase64</td>
<td>boolean</td>
<td>Specifies whether to use Base64 encoding.</td>
</tr>
<tr>
<td>kinesis</td>
<td>KinesisAction</td>
<td>Write data to an Amazon Kinesis stream.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the Amazon Kinesis stream.</td>
</tr>
<tr>
<td>streamName</td>
<td>string</td>
<td>The name of the Amazon Kinesis stream.</td>
</tr>
<tr>
<td>partitionKey</td>
<td>string</td>
<td>The partition key.</td>
</tr>
<tr>
<td>republish</td>
<td>RepublishAction</td>
<td>Publish to another MQTT topic.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>topic</td>
<td>string</td>
<td>The name of the MQTT topic.</td>
</tr>
<tr>
<td>s3</td>
<td>S3Action</td>
<td>Write to an Amazon S3 bucket.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>bucketName</td>
<td>string</td>
<td>The Amazon S3 bucket.</td>
</tr>
<tr>
<td>key</td>
<td>string</td>
<td>The object key.</td>
</tr>
<tr>
<td>cannedAcl</td>
<td>string</td>
<td>The Amazon S3 canned ACL that controls access to the object identified by the object key. For more information, see S3 canned ACLs. enum: private</td>
</tr>
<tr>
<td>firehose</td>
<td>FirehoseAction</td>
<td>Write to an Amazon Kinesis Firehose stream.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role that grants access to the Amazon Kinesis Firehose stream.</td>
</tr>
<tr>
<td>deliveryStreamName</td>
<td>string</td>
<td>The delivery stream name.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| separator             | string              | A character separator that will be used to separate records written to the Firehose stream. Valid values are: 
\n' (newline), \t (tab), ' (Windows newline), , (comma). |
<p>| cloudwatchMetric      | CloudwatchMetricAction | Capture a CloudWatch metric.                                               |
| roleArn               | string              | The IAM role that allows access to the CloudWatch metric.                   |
| metricNamespace       | string              | The CloudWatch metric namespace name.                                       |
| metricName            | string              | The CloudWatch metric name.                                                |
| metricValue           | string              | The CloudWatch metric value.                                               |
| metricUnit            | string              | The metric unit supported by CloudWatch.                                   |
| metricTimestamp       | string              | An optional Unix timestamp.                                                |
| cloudwatchAlarm       | CloudwatchAlarmAction | Change the state of a CloudWatch alarm.                                    |
| roleArn               | string              | The IAM role that allows access to the CloudWatch alarm.                    |
| alarmName             | string              | The CloudWatch alarm name.                                                 |
| stateReason           | string              | The reason for the alarm change.                                           |
| stateValue            | string              | The value of the alarm state. Acceptable values are: OK, ALARM, INSUFFICIENT_DATA. |
| elasticsearch         | ElasticsearchAction | Write data to an Amazon Elasticsearch Service domain.                      |
| roleArn               | string              | The IAM role ARN that has access to Elasticsearch.                         |
| endpoint              | string              | The endpoint of your Elasticsearch domain.                                 |
| index                 | string              | The Elasticsearch index where you want to store your data.                  |
| type                  | string              | The type of document you are storing.                                      |
| id                    | string              | The unique identifier for the document you are storing.                     |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>salesforce</td>
<td>SalesforceAction</td>
<td>Send a message to a Salesforce IoT Cloud Input Stream.</td>
</tr>
<tr>
<td>token</td>
<td>string</td>
<td>The token used to authenticate access to the Salesforce IoT Cloud Input Stream. The token is available from the Salesforce IoT Cloud platform after creation of the Input Stream.</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>The URL exposed by the Salesforce IoT Cloud Input Stream. The URL is available from the Salesforce IoT Cloud platform after creation of the Input Stream.</td>
</tr>
<tr>
<td>iotAnalytics</td>
<td>IotAnalyticsAction</td>
<td>Sends message data to an AWS IoT Analytics channel.</td>
</tr>
<tr>
<td>channelArn</td>
<td>string</td>
<td>(deprecated) The ARN of the IoT Analytics channel to which message data will be sent.</td>
</tr>
<tr>
<td>channelName</td>
<td>string</td>
<td>The name of the IoT Analytics channel to which message data will be sent.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role which has a policy that grants IoT Analytics permission to send message data via IoT Analytics (iotanalytics:BatchPutMessage).</td>
</tr>
<tr>
<td>stepFunctions</td>
<td>StepFunctionsAction</td>
<td>Starts execution of a Step Functions state machine.</td>
</tr>
<tr>
<td>executionNamePrefix</td>
<td>string</td>
<td>(Optional) A name will be given to the state machine execution consisting of this prefix followed by a UUID. Step Functions automatically creates a unique name for each state machine execution if one is not provided.</td>
</tr>
<tr>
<td>stateMachineName</td>
<td>string</td>
<td>The name of the Step Functions state machine whose execution will be started.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants IoT permission to start execution of a state machine (&quot;Action&quot;:&quot;states:StartExecution&quot;).</td>
</tr>
</tbody>
</table>
### CreateTopicRule

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleDisabled</td>
<td>boolean</td>
<td>Specifies whether the rule is disabled.</td>
</tr>
<tr>
<td>awsIoTSqlVersion</td>
<td>string</td>
<td>The version of the SQL rules engine to use when evaluating the rule.</td>
</tr>
<tr>
<td>errorAction</td>
<td>Action</td>
<td>The action to take when an error occurs.</td>
</tr>
<tr>
<td>dynamoDB</td>
<td>DynamoDBAction</td>
<td>Write to a DynamoDB table.</td>
</tr>
<tr>
<td>tableName</td>
<td>string</td>
<td>The name of the DynamoDB table.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the DynamoDB table.</td>
</tr>
<tr>
<td>operation</td>
<td>string</td>
<td>The type of operation to be performed. This follows the substitution template, so it can be $operation, but the substitution must result in one of the following: INSERT, UPDATE, or DELETE.</td>
</tr>
<tr>
<td>hashKeyField</td>
<td>string</td>
<td>The hash key name.</td>
</tr>
<tr>
<td>hashKeyValue</td>
<td>string</td>
<td>The hash key value.</td>
</tr>
<tr>
<td>hashKeyType</td>
<td>string</td>
<td>The hash key type. Valid values are &quot;STRING&quot; or &quot;NUMBER&quot;</td>
</tr>
<tr>
<td>rangeKeyField</td>
<td>string</td>
<td>The range key name.</td>
</tr>
<tr>
<td>rangeKeyValue</td>
<td>string</td>
<td>The range key value.</td>
</tr>
<tr>
<td>rangeKeyType</td>
<td>string</td>
<td>The range key type. Valid values are &quot;STRING&quot; or &quot;NUMBER&quot;</td>
</tr>
<tr>
<td>payloadField</td>
<td>string</td>
<td>The action payload. This name can be customized.</td>
</tr>
<tr>
<td>dynamoDBv2</td>
<td>DynamoDBv2Action</td>
<td>Write to a DynamoDB table. This is a new version of the DynamoDB action. It allows you to write each attribute in an MQTT message payload into a separate DynamoDB column.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the DynamoDB table.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>putItem</td>
<td>PutItemInput</td>
<td>Specifies the DynamoDB table to which the message data will be written. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{ &quot;dynamodbv2&quot;: { &quot;roleArn&quot;: &quot;aws:iam:12341251:my-role&quot; &quot;putItem&quot;: { &quot;tableName&quot;: &quot;my-table&quot; } } }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Each attribute in the message payload will be written to a separate column in the DynamoDB database.</td>
</tr>
<tr>
<td>tableName</td>
<td>string</td>
<td>The table where the message data will be written.</td>
</tr>
<tr>
<td>lambda</td>
<td>LambdaAction</td>
<td>Invoke a Lambda function.</td>
</tr>
<tr>
<td>functionArn</td>
<td>string</td>
<td>The ARN of the Lambda function.</td>
</tr>
<tr>
<td>sns</td>
<td>SnsAction</td>
<td>Publish to an Amazon SNS topic.</td>
</tr>
<tr>
<td>targetArn</td>
<td>string</td>
<td>The ARN of the SNS topic.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>messageFormat</td>
<td>string</td>
<td>(Optional) The message format of the message to publish. Accepted values are &quot;JSON&quot; and &quot;RAW&quot;. The default value of the attribute is &quot;RAW&quot;. SNS uses this setting to determine if the payload should be parsed and relevant platform-specific bits of the payload should be extracted. To read more about SNS message formats, see <a href="http://docs.aws.amazon.com/sns/latest/dg/json-formats.html">http://docs.aws.amazon.com/sns/latest/dg/json-formats.html</a> refer to their official documentation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: RAW</td>
</tr>
<tr>
<td>sqs</td>
<td>SqsAction</td>
<td>Publish to an Amazon SQS queue.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>queueUrl</td>
<td>string</td>
<td>The URL of the Amazon SQS queue.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>useBase64</td>
<td>boolean</td>
<td>Specifies whether to use Base64 encoding.</td>
</tr>
<tr>
<td>kinesis</td>
<td>KinesisAction</td>
<td>Write data to an Amazon Kinesis stream.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the Amazon Kinesis stream.</td>
</tr>
<tr>
<td>streamName</td>
<td>string</td>
<td>The name of the Amazon Kinesis stream.</td>
</tr>
<tr>
<td>partitionKey</td>
<td>string</td>
<td>The partition key.</td>
</tr>
<tr>
<td>republish</td>
<td>RepublishAction</td>
<td>Publish to another MQTT topic.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>topic</td>
<td>string</td>
<td>The name of the MQTT topic.</td>
</tr>
<tr>
<td>s3</td>
<td>S3Action</td>
<td>Write to an Amazon S3 bucket.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>bucketName</td>
<td>string</td>
<td>The Amazon S3 bucket.</td>
</tr>
<tr>
<td>key</td>
<td>string</td>
<td>The object key.</td>
</tr>
<tr>
<td>cannedAcl</td>
<td>string</td>
<td>The Amazon S3 canned ACL that controls access to the object identified by</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the object key.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information, see <a href="#">S3 canned ACLs</a>.</td>
</tr>
<tr>
<td>firehose</td>
<td>FirehoseAction</td>
<td>Write to an Amazon Kinesis Firehose stream.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role that grants access to the Amazon Kinesis Firehose stream.</td>
</tr>
<tr>
<td>deliveryStreamName</td>
<td>string</td>
<td>The delivery stream name.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>separator</td>
<td>string</td>
<td>A character separator that will be used to separate records written to the Firehose stream. Valid values are: \n (newline), \t (tab), \r\n (Windows newline), , (comma).</td>
</tr>
<tr>
<td>cloudwatchMetric</td>
<td>CloudwatchMetricAction</td>
<td>Capture a CloudWatch metric.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role that allows access to the CloudWatch metric.</td>
</tr>
<tr>
<td>metricNamespace</td>
<td>string</td>
<td>The CloudWatch metric namespace name.</td>
</tr>
<tr>
<td>metricName</td>
<td>string</td>
<td>The CloudWatch metric name.</td>
</tr>
<tr>
<td>metricValue</td>
<td>string</td>
<td>The CloudWatch metric value.</td>
</tr>
<tr>
<td>metricUnit</td>
<td>string</td>
<td>The metric unit supported by CloudWatch.</td>
</tr>
<tr>
<td>metricTimestamp</td>
<td>string</td>
<td>An optional Unix timestamp.</td>
</tr>
<tr>
<td>cloudwatchAlarm</td>
<td>CloudwatchAlarmAction</td>
<td>Change the state of a CloudWatch alarm.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role that allows access to the CloudWatch alarm.</td>
</tr>
<tr>
<td>alarmName</td>
<td>string</td>
<td>The CloudWatch alarm name.</td>
</tr>
<tr>
<td>stateReason</td>
<td>string</td>
<td>The reason for the alarm change.</td>
</tr>
<tr>
<td>stateValue</td>
<td>string</td>
<td>The value of the alarm state. Acceptable values are: OK, ALARM, INSUFFICIENT_DATA.</td>
</tr>
<tr>
<td>elasticsearch</td>
<td>ElasticsearchAction</td>
<td>Write data to an Amazon Elasticsearch Service domain.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role ARN that has access to Elasticsearch.</td>
</tr>
<tr>
<td>endpoint</td>
<td>string</td>
<td>The endpoint of your Elasticsearch domain.</td>
</tr>
<tr>
<td>index</td>
<td>string</td>
<td>The Elasticsearch index where you want to store your data.</td>
</tr>
<tr>
<td>type</td>
<td>string</td>
<td>The type of document you are storing.</td>
</tr>
<tr>
<td>id</td>
<td>string</td>
<td>The unique identifier for the document you are storing.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>salesforce</td>
<td>SalesforceAction</td>
<td>Send a message to a Salesforce IoT Cloud Input Stream.</td>
</tr>
<tr>
<td>token</td>
<td>string</td>
<td>The token used to authenticate access to the Salesforce IoT Cloud Input Stream. The token is available from the Salesforce IoT Cloud platform after creation of the Input Stream.</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>The URL exposed by the Salesforce IoT Cloud Input Stream. The URL is available from the Salesforce IoT Cloud platform after creation of the Input Stream.</td>
</tr>
<tr>
<td>iotAnalytics</td>
<td>IotAnalyticsAction</td>
<td>Sends message data to an AWS IoT Analytics channel.</td>
</tr>
<tr>
<td>channelArn</td>
<td>string</td>
<td>(deprecated) The ARN of the IoT Analytics channel to which message data will be sent.</td>
</tr>
<tr>
<td>channelName</td>
<td>string</td>
<td>The name of the IoT Analytics channel to which message data will be sent.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role which has a policy that grants IoT Analytics permission to send message data via IoT Analytics (iotanalytics:BatchPutMessage).</td>
</tr>
<tr>
<td>stepFunctions</td>
<td>StepFunctionsAction</td>
<td>Starts execution of a Step Functions state machine.</td>
</tr>
<tr>
<td>executionNamePrefix</td>
<td>string</td>
<td>(Optional) A name will be given to the state machine execution consisting of this prefix followed by a UUID. Step Functions automatically creates a unique name for each state machine execution if one is not provided.</td>
</tr>
<tr>
<td>stateMachineName</td>
<td>string</td>
<td>The name of the Step Functions state machine whose execution will be started.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants IoT permission to start execution of a state machine (&quot;Action&quot;:&quot;states:StartExecution&quot;).</td>
</tr>
</tbody>
</table>
DeleteAccountAuditConfiguration

Restores the default settings for Device Defender audits for this account. Any configuration data you entered is deleted and all audit checks are reset to disabled.

https

Request syntax:

```
DELETE /audit/configuration?deleteScheduledAudits=deleteScheduledAudits
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deleteScheduledAudits</td>
<td>DeleteScheduledAudits</td>
<td>no</td>
<td>If true, all scheduled audits are deleted.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.
HTTP response code: 404
ThrottlingException
The rate exceeds the limit.
HTTP response code: 429
InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

cli

Synopsis:

```
aws iot delete-account-audit-configuration \ 
    [--delete-scheduled-audits | --no-delete-scheduled-audits] \ 
    [--cli-input-json <value>] \ 
    [--generate-cli-skeleton]
```

cli-input-json format:

```
{
    "deleteScheduledAudits": "boolean"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deleteScheduledAudits</td>
<td>boolean</td>
<td>If true, all scheduled audits are deleted.</td>
</tr>
</tbody>
</table>

Output:
None

Errors:

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceNotFoundException
The specified resource does not exist.

ThrottlingException
The rate exceeds the limit.

InternalFailureException
An unexpected error has occurred.
DeleteAuthorizer

Deletes an authorizer.

https

Request syntax:

DELETE /authorizer/authorizerName

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>AuthorizerName</td>
<td>yes</td>
<td>The name of the authorizer to delete.</td>
</tr>
</tbody>
</table>

Errors:

DeleteConflictException
   You can't delete the resource because it is attached to one or more resources.
   HTTP response code: 409

ResourceNotFoundException
   The specified resource does not exist.
   HTTP response code: 404

InvalidRequestException
   The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
   HTTP response code: 400

ThrottlingException
   The rate exceeds the limit.
   HTTP response code: 429

UnauthorizedException
   You are not authorized to perform this operation.
   HTTP response code: 401

ServiceUnavailableException
   The service is temporarily unavailable.
   HTTP response code: 503

InternalFailureException
   An unexpected error has occurred.
HTTP response code: 500

cli

Synopsis:

```
aws iot delete-authorizer \
   --authorizer-name <value> \ 
   [--cli-input-json <value>] \ 
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "authorizerName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>string</td>
<td>The name of the authorizer to delete.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w=,@-]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

None

Errors:

DeleteConflictException

You can't delete the resource because it is attached to one or more resources.

ResourceNotFoundException

The specified resource does not exist.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.
DeleteCACertificate

Deletes a registered CA certificate.

https

Request syntax:

DELETE /cacertificate/caCertificateId

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>Certificateld</td>
<td>yes</td>
<td>The ID of the certificate to delete. (The last part of the certificate ARN contains the certificate ID.)</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

CertificateStateException

The certificate operation is not allowed.

HTTP response code: 406

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

ResourceNotFoundException

The specified resource does not exist.
HTTP response code: 404

cli

Synopsis:

```
aws iot delete-ca-certificate \
  --certificate-id <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "certificateId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>string</td>
<td>The ID of the certificate to delete. (The last part of the certificate ARN contains the certificate ID.)</td>
</tr>
</tbody>
</table>

Output:

None

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

CertificateStateException

The certificate operation is not allowed.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

ResourceNotFoundException

The specified resource does not exist.
DeleteCertificate

Deletes the specified certificate.

A certificate cannot be deleted if it has a policy attached to it or if its status is set to ACTIVE. To delete a certificate, first use the DetachPrincipalPolicy API to detach all policies. Next, use the UpdateCertificate API to set the certificate to the INACTIVE status.

https

Request syntax:

DELETE /certificates/certificateId?forceDelete=forceDelete

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>CertificateId</td>
<td>yes</td>
<td>The ID of the certificate. (The last part of the certificate ARN contains the certificate ID.)</td>
</tr>
<tr>
<td>forceDelete</td>
<td>ForceDelete</td>
<td>no</td>
<td>Forces a certificate request to be deleted.</td>
</tr>
</tbody>
</table>

Errors:

CertificateStateException

The certificate operation is not allowed.

HTTP response code: 406

DeleteConflictException

You can't delete the resource because it is attached to one or more resources.

HTTP response code: 409

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401
ServiceUnavailableException
The service is temporarily unavailable.
HTTP response code: 503

InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

ResourceNotFoundException
The specified resource does not exist.
HTTP response code: 404

cli

Synopsis:

```
aws iot delete-certificate \
  --certificate-id <value> \
  [--force-delete | --no-force-delete] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "certificateId": "string",
  "forceDelete": "boolean"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>string</td>
<td>The ID of the certificate. (The last part of the certificate ARN contains the certificate ID.)</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:64</td>
<td>pattern: (0x)?[a-fA-F0-9]+</td>
</tr>
<tr>
<td>forceDelete</td>
<td>boolean</td>
<td>Forces a certificate request to be deleted.</td>
</tr>
</tbody>
</table>

Output:

None

Errors:

CertificateStateException
The certificate operation is not allowed.

DeleteConflictException
You can't delete the resource because it is attached to one or more resources.
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

ResourceNotFoundException

The specified resource does not exist.

DeleteJob

Deletes a job and its related job executions.

Deleting a job may take time, depending on the number of job executions created for the job and various other factors. While the job is being deleted, the status of the job will be shown as "DELETION_IN_PROGRESS". Attempting to delete or cancel a job whose status is already "DELETION_IN_PROGRESS" will result in an error.

Only 10 jobs may have status "DELETION_IN_PROGRESS" at the same time, or a LimitExceededException will occur.

https

Request syntax:

DELETE /jobs/jobId?force=force

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>JobId</td>
<td>yes</td>
<td>The ID of the job to be deleted. After a job deletion is completed, you may reuse this jobId when you create a new job. However, this is not recommended, and you must ensure that your devices are not using the jobId to refer to the deleted job.</td>
</tr>
</tbody>
</table>
DeleteJob

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>force</td>
<td>ForceFlag</td>
<td>no</td>
<td>(Optional) When true, you can delete a job which is &quot;IN_PROGRESS&quot;. Otherwise, you can only delete a job which is in a terminal state (&quot;COMPLETED&quot; or &quot;CANCELED&quot;) or an exception will occur. The default is false.</td>
</tr>
</tbody>
</table>

**Note**
Deleting a job which is "IN_PROGRESS", will cause a device which is executing the job to be unable to access job information or update the job execution status. Use caution and ensure that each device executing a job which is deleted is able to recover to a valid state.

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**InvalidStateTransitionException**

An update attempted to change the job execution to a state that is invalid because of the job execution's current state (for example, an attempt to change a request in state SUCCESS to state IN_PROGRESS). In this case, the body of the error message also contains the executionState field.

HTTP response code: 409

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404
LimitExceededException

A limit has been exceeded.

HTTP response code: 410

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

cli

Synopsis:

    aws iot delete-job \
    --job-id <value> \
    [--force | --no-force] \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]

cli-input-json format:

    {
        "jobId": "string",
        "force": "boolean"
    }

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The ID of the job to be deleted. After a job deletion is completed, you may reuse this jobId when you create a new job. However, this is not recommended, and you must ensure that your devices are not using the jobId to refer to the deleted job.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>force</td>
<td>boolean</td>
<td>(Optional) When true, you can delete a job which is &quot;IN_PROGRESS&quot;. Otherwise, you can only delete a job which is in a terminal state (&quot;COMPLETED&quot; or &quot;CANCELED&quot;) or an exception will occur. The default is false.</td>
</tr>
</tbody>
</table>
DeleteJobExecution

Deleted a job which is "IN_PROGRESS", will cause a device which is executing the job to be unable to access job information or update the job execution status. Use caution and ensure that each device executing a job which is deleted is able to recover to a valid state.

Output:
None

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

InvalidStateException

An update attempted to change the job execution to a state that is invalid because of the job execution’s current state (for example, an attempt to change a request in state SUCCESS to state IN_PROGRESS). In this case, the body of the error message also contains the executionState field.

ResourceNotFoundException

The specified resource does not exist.

LimitExceededException

A limit has been exceeded.

ThrottlingException

The rate exceeds the limit.

ServiceUnavailableException

The service is temporarily unavailable.

DeleteJobExecution

Deletes a job execution.

https

Request syntax:
DELETE /things/thingName/jobs/jobId/execuusernamectionNumber/execuusernamectionNumber?force=force

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>JobId</td>
<td>yes</td>
<td>The ID of the job whose execution on a particular device will be deleted.</td>
</tr>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing whose job execution will be deleted.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>ExecutionNumber</td>
<td>yes</td>
<td>The ID of the job execution to be deleted. The executionNumber refers to the execution of a particular job on a particular device. Note that once a job execution is deleted, the executionNumber may be reused by IoT, so be sure you get and use the correct value here.</td>
</tr>
<tr>
<td>force</td>
<td>ForceFlag</td>
<td>no</td>
<td>(Optional) When true, you can delete a job execution which is &quot;IN_PROGRESS&quot;. Otherwise, you can only delete a job execution which is in a terminal state (&quot;SUCCEEDED&quot;, &quot;FAILED&quot;, &quot;REJECTED&quot;, &quot;REMOVED&quot; or &quot;CANCELED&quot;) or an exception will occur. The default is false. <strong>Note</strong> Deleting a job execution which is &quot;IN_PROGRESS&quot;, will cause the device to be unable to access job information or update the job execution status. Use caution and</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Req?</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ensure that the device is able to recover to a valid state.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**InvalidStateTransitionException**

An update attempted to change the job execution to a state that is invalid because of the job execution's current state (for example, an attempt to change a request in state SUCCESS to state IN_PROGRESS). In this case, the body of the error message also contains the executionState field.

HTTP response code: 409

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**ServiceUnavailableException**

The service is temporarily unavailable.

HTTP response code: 503

**cli**

**Synopsis:**

```bash
aws iot delete-job-execution \
  --job-id <value> \
  --thing-name <value> \
  --execution-number <value> \
  [--force | --no-force] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
  "jobId": "string",
  "thingName": "string",
  "executionNumber": "long",
...}
```
"force": "boolean"
}

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The ID of the job whose execution on a particular device will be deleted.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9_]+</td>
<td></td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing whose job execution will be deleted.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>executionNumber</td>
<td>long</td>
<td>The ID of the job execution to be deleted. The executionNumber refers to the execution of a particular job on a particular device. Note that once a job execution is deleted, the executionNumber may be reused by IoT, so be sure you get and use the correct value here.</td>
</tr>
<tr>
<td>force</td>
<td>boolean</td>
<td>(Optional) When true, you can delete a job execution which is &quot;IN_PROGRESS&quot;. Otherwise, you can only delete a job execution which is in a terminal state (&quot;SUCCEEDED&quot;, &quot;FAILED&quot;, &quot;REJECTED&quot;, &quot;REMOVED&quot; or &quot;CANCELED&quot;) or an exception will occur. The default is false. <strong>Note</strong> Deleting a job execution which is &quot;IN_PROGRESS&quot;, will cause the device to be unable to access job information or update the job execution status. Use caution and ensure that the device is able to recover to a valid state.</td>
</tr>
</tbody>
</table>

**Output:**

None

**Errors:**
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

InvalidStateTransitionException

An update attempted to change the job execution to a state that is invalid because of the job execution's current state (for example, an attempt to change a request in state SUCCESS to state IN_PROGRESS). In this case, the body of the error message also contains the executionState field.

ResourceNotFoundException

The specified resource does not exist.

ThrottlingException

The rate exceeds the limit.

ServiceUnavailableException

The service is temporarily unavailable.

DeleteOTAUpdate

Delete an OTA update.

https

Request syntax:

DELETE /otaUpdates/otaUpdateId

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>otaUpdateId</td>
<td>OTAUpdateId</td>
<td>yes</td>
<td>The OTA update ID to delete.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.
HTTP response code: 429
UnauthorizedException
You are not authorized to perform this operation.

HTTP response code: 401
InternalFailureException
An unexpected error has occurred.

HTTP response code: 500
ServiceUnavailableException
The service is temporarily unavailable.

HTTP response code: 503

cli

Synopsis:

```bash
aws iot delete-ota-update \
  --ota-update-id <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "otaUpdateId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>otaUpdateId</td>
<td>string</td>
<td>The OTA update ID to delete.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

None

Errors:

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceNotFoundException
The specified resource does not exist.
DeletePolicy

Deletes the specified policy.

A policy cannot be deleted if it has non-default versions or it is attached to any certificate.

To delete a policy, use the DeletePolicyVersion API to delete all non-default versions of the policy; use the DetachPrincipalPolicy API to detach the policy from any certificate; and then use the DeletePolicy API to delete the policy.

When a policy is deleted using DeletePolicy, its default version is deleted with it.

https

Request syntax:

```
DELETE /policies/policyName
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>yes</td>
<td>The name of the policy to delete.</td>
</tr>
</tbody>
</table>

Errors:

DeleteConflictException

You can't delete the resource because it is attached to one or more resources.

HTTP response code: 409

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
HTTP response code: 400
ThrottlingException
The rate exceeds the limit.

HTTP response code: 429
UnauthorizedException
You are not authorized to perform this operation.

HTTP response code: 401
ServiceUnavailableException
The service is temporarily unavailable.

HTTP response code: 503
InternalFailureException
An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

aws iot delete-policy \
  --policy-name <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]

cli-input-json format:

{
  "policyName": "string"
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>string</td>
<td>The name of the policy to delete.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [w+=,.@-]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:
None

Errors:

DeleteConflictException
You can't delete the resource because it is attached to one or more resources.
ResourceNotFoundException

The specified resource does not exist.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

DeletePolicyVersion

Deletes the specified version of the specified policy. You cannot delete the default version of a policy using this API. To delete the default version of a policy, use DeletePolicy. To find out which version of a policy is marked as the default version, use ListPolicyVersions.

https

Request syntax:

```
DELETE /policies/policyName/version/policyVersionId
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>yes</td>
<td>The name of the policy.</td>
</tr>
<tr>
<td>policyVersionId</td>
<td>PolicyVersionId</td>
<td>yes</td>
<td>The policy version ID.</td>
</tr>
</tbody>
</table>

**Errors:**

DeleteConflictException

You can't delete the resource because it is attached to one or more resources.

HTTP response code: 409

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```bash
aws iot delete-policy-version \
  --policy-name <value> \
  --policy-version-id <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "policyName": "string",
  "policyVersionId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>string</td>
<td>length= max:128 min:1 pattern: [w+=,.@-]+</td>
</tr>
<tr>
<td>policyVersionId</td>
<td>string</td>
<td>pattern: [0-9]+</td>
</tr>
</tbody>
</table>
DeleteRegistrationCode

Deletes a CA certificate registration code.

https

Request syntax:

```
DELETE /registrationcode
```

Errors:

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

UnauthorizedException

You are not authorized to perform this operation.
HTTP response code: 401
ServiceUnavailableException
The service is temporarily unavailable.

HTTP response code: 503
InternalFailureException
An unexpected error has occurred.

HTTP response code: 500
cli

Synopsis:

```
aws iot delete-registration-code
   [--cli-input-json <value>]
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
}
```

Output:
None

Errors:

ThrottlingException
The rate exceeds the limit.

ResourceNotFoundException
The specified resource does not exist.

UnauthorizedException
You are not authorized to perform this operation.

ServiceUnavailableException
The service is temporarily unavailable.

InternalFailureException
An unexpected error has occurred.

DeleteRoleAlias

Deletes a role alias

https

Request syntax:
DELETE /role-aliases/roleAlias

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleAlias</td>
<td>RoleAlias</td>
<td>yes</td>
<td>The role alias to delete.</td>
</tr>
</tbody>
</table>

Errors:

DeleteConflictException
You can't delete the resource because it is attached to one or more resources.
HTTP response code: 409

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
HTTP response code: 400

ThrottlingException
The rate exceeds the limit.
HTTP response code: 429

UnauthorizedException
You are not authorized to perform this operation.
HTTP response code: 401

ServiceUnavailableException
The service is temporarily unavailable.
HTTP response code: 503

InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

ResourceNotFoundException
The specified resource does not exist.
HTTP response code: 404

cli

Synopsis:

```
aws iot delete-role-alias \   
  --role-alias <value> \   
  [--cli-input-json <value>] \   
  [--generate-cli-skeleton]
```
DeleteScheduledAudit

Deletes a scheduled audit.

Request syntax:

```
DELETE /audit/scheduledaudits/scheduledAuditName
```
**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditName</td>
<td>ScheduledAuditName</td>
<td>yes</td>
<td>The name of the scheduled audit you want to delete.</td>
</tr>
</tbody>
</table>

**Errors:**

*InvalidRequestException*

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

*ResourceNotFoundException*

The specified resource does not exist.

HTTP response code: 404

*ThrottlingException*

The rate exceeds the limit.

HTTP response code: 429

*InternalFailureException*

An unexpected error has occurred.

HTTP response code: 500

**cli**

**Synopsis:**

```
aws iot delete-scheduled-audit \
   --scheduled-audit-name <value> \
   [-cli-input-json <value>] \
   [--generate-cli-skeleton]
```

**cli-input-json format:**

```
{
   "scheduledAuditName": "string"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditName</td>
<td>string</td>
<td>The name of the scheduled audit you want to delete.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9_]+</td>
<td></td>
</tr>
</tbody>
</table>
Output:
None

Errors:

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceNotFoundException
The specified resource does not exist.

ThrottlingException
The rate exceeds the limit.

InternalFailureException
An unexpected error has occurred.

DeleteSecurityProfile

Deletes a Device Defender security profile.

https

Request syntax:

```
DELETE /security-profiles/securityProfileName?expectedVersion=expectedVersion
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>yes</td>
<td>The name of the security profile to be deleted.</td>
</tr>
<tr>
<td>expectedVersion</td>
<td>OptionalVersion</td>
<td>no</td>
<td>The expected version of the security profile. A new version is generated whenever the security profile is updated. If you specify a value that is different than the actual version, a VersionConflictException is thrown.</td>
</tr>
</tbody>
</table>

Errors:
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

VersionConflictException

An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

HTTP response code: 409

cli

Synopsis:

```
aws iot delete-security-profile
   --security-profile-name <value> \
   [--expected-version <value>] \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "securityProfileName": "string",
   "expectedVersion": "long"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name of the security profile to be deleted.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_:]+</td>
<td></td>
</tr>
<tr>
<td>expectedVersion</td>
<td>long</td>
<td>The expected version of the security profile. A new version is generated whenever the security profile is updated. If you specify a value that is different than the actual version, a VersionConflictException is thrown.</td>
</tr>
</tbody>
</table>
Output:
None

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

VersionConflictException

An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

DeleteStream

Deletes a stream.

https

Request syntax:

DELETE /streams/streamId

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streamId</td>
<td>StreamId</td>
<td>yes</td>
<td>The stream ID.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

DeleteConflictException

You can't delete the resource because it is attached to one or more resources.

HTTP response code: 409

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
HTTP response code: 400
ThrottlingException
The rate exceeds the limit.

HTTP response code: 429
UnauthorizedException
You are not authorized to perform this operation.

HTTP response code: 401
ServiceUnavailableException
The service is temporarily unavailable.

HTTP response code: 503
InternalFailureException
An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot delete-stream \
   --stream-id <value> \ 
   [--cli-input-json <value>] \ 
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "streamId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streamId</td>
<td>string</td>
<td>The stream ID.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9_-]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:
None

Errors:

ResourceNotFoundException
The specified resource does not exist.
DeleteThing

Deletes the specified thing.

https

Request syntax:

DELETE /things/thingName?expectedVersion=expectedVersion

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing to delete.</td>
</tr>
<tr>
<td>expectedVersion</td>
<td>OptionalVersion</td>
<td>no</td>
<td>The expected version of the thing record in the registry. If the version of the record in the registry does not match the expected version specified in the request, the DeleteThing request is rejected with a VersionConflictException.</td>
</tr>
</tbody>
</table>

Errors:
ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

VersionConflictException

An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

HTTP response code: 409

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot delete-thing
   --thing-name <value> \
   [--expected-version <value>] \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "thingName": "string",
   "expectedVersion": "long"
}
```
**DeleteThingGroup**

Deletes a thing group.

**https**

**Request syntax:**

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing to delete.</td>
</tr>
<tr>
<td></td>
<td>length: max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>expectedVersion</td>
<td>long</td>
<td>The expected version of the thing record in the registry. If the version of the record in the registry does not match the expected version specified in the request, the DeleteThing request is rejected with a VersionConflictException.</td>
</tr>
</tbody>
</table>

Output:
None

**Errors:**

- **ResourceNotFoundException**
  The specified resource does not exist.

- **VersionConflictException**
  An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

- **InvalidRequestException**
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ThrottlingException**
  The rate exceeds the limit.

- **UnauthorizedException**
  You are not authorized to perform this operation.

- **ServiceUnavailableException**
  The service is temporarily unavailable.

- **InternalFailureException**
  An unexpected error has occurred.
DELETE /thing-groups/<thingGroupName>?expectedVersion=<expectedVersion>

### URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>ThingGroupName</td>
<td>yes</td>
<td>The name of the thing group to delete.</td>
</tr>
<tr>
<td>expectedVersion</td>
<td>OptionalVersion</td>
<td>no</td>
<td>The expected version of the thing group to delete.</td>
</tr>
</tbody>
</table>

### Errors:

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**VersionConflictException**

An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

HTTP response code: 409

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

### cli

**Synopsis:**

```bash
aws iot delete-thing-group \
    --thing-group-name <value> \
    [--expected-version <value>] \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

#### cli-input-json format:

```json
{
    "thingGroupName": "string",
    "expectedVersion": "long"
}
```
DeleteThingShadow

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>string</td>
<td>The name of the thing group to delete.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>expectedVersion</td>
<td>long</td>
<td>The expected version of the thing group to delete.</td>
</tr>
</tbody>
</table>

Output:

None

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

VersionConflictException

An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

DeleteThingShadow

Deletes the shadow for the specified thing.

For more information, see DeleteThingShadow in the AWS IoT Developer Guide.

https

Request syntax:

```
DELETE /things/thingName/shadow
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing.</td>
</tr>
</tbody>
</table>

Response syntax:
Content-type: application/json
{
 "payload": "blob"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>payload</td>
<td>JsonDocument</td>
<td>yes</td>
<td>The state information, in JSON format.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

MethodNotAllowedException

The specified combination of HTTP verb and URI is not supported.

HTTP response code: 405

UnsupportedDocumentEncodingException

The encoding is not supported.

HTTP response code: 415
cli

Synopsis:

```
aws iot-data delete-thing-shadow \
  --thing-name <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "thingName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```
{
  "payload": "blob"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>payload</td>
<td>blob</td>
<td>The state information, in JSON format.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException

The specified resource does not exist.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.
DeleteThingType

Deletes the specified thing type. You cannot delete a thing type if it has things associated with it. To delete a thing type, first mark it as deprecated by calling DeprecateThingType, then remove any associated things by calling UpdateThing to change the thing type on any associated thing, and finally use DeleteThingType to delete the thing type.

https

Request syntax:

```
DELETE /thing-types/thingTypeName
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>ThingTypeName</td>
<td>yes</td>
<td>The name of the thing type.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.
HTTP response code: 401
ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503
InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot delete-thing-type
   --thing-type-name <value> \n    [--cli-input-json <value>] \n    [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "thingTypeName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>string</td>
<td>The name of the thing type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>length- max:128 min:1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
</tr>
</tbody>
</table>

Output:

None

Errors:

ResourceNotFoundException

The specified resource does not exist.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.
ServiceUnavailableException
The service is temporarily unavailable.

InternalFailureException
An unexpected error has occurred.

DeleteTopicRule

Deletes the rule.

https

Request syntax:

```
DELETE /rules/ruleName
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleName</td>
<td>RuleName</td>
<td>no</td>
<td>The name of the rule.</td>
</tr>
</tbody>
</table>

Errors:

InternalException
An unexpected error has occurred.
HTTP response code: 500

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
HTTP response code: 400

ServiceUnavailableException
The service is temporarily unavailable.
HTTP response code: 503

UnauthorizedException
You are not authorized to perform this operation.
HTTP response code: 401

cli

Synopsis:

```
aws iot delete-topic-rule
  [--rule-name <value>]
  [--cli-input-json <value>]
  [--generate-cli-skeleton]
```
DeleteV2LoggingLevel

Deletes a logging level.

Request syntax:

DELETE /v2LoggingLevel?targetName=targetName&targetType=targetType

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targetType</td>
<td>LogTargetType</td>
<td>yes</td>
<td>The type of resource for which you are configuring logging. Must be THING_Group.</td>
</tr>
</tbody>
</table>
### Name | Type | Req? | Description
--- | --- | --- | ---
targetName | LogTargetName | yes | The name of the resource for which you are configuring logging.

**Errors:**

**InternalException**

An unexpected error has occurred.

HTTP response code: 500

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ServiceUnavailableException**

The service is temporarily unavailable.

HTTP response code: 503

**cli**

**Synopsis:**

```bash
aws iot delete-v2-logging-level \
    --target-type <value> \
    --target-name <value>  \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
    "targetType": "string",
    "targetName": "string"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targetType</td>
<td>string</td>
<td>The type of resource for which you are configuring logging. Must be THING_Group. enum: DEFAULT</td>
</tr>
<tr>
<td>targetName</td>
<td>string</td>
<td>The name of the resource for which you are configuring logging.</td>
</tr>
</tbody>
</table>
DeprecateThingType

Deprecates a thing type. You can not associate new things with deprecated thing type.

**https**

**Request syntax:**

```plaintext
POST /thing-types/thingTypeName/deprecate
Content-type: application/json

{
   "undoDeprecate": "boolean"
}
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>ThingTypeName</td>
<td>yes</td>
<td>The name of the thing type to deprecate.</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>undoDeprecate</td>
<td>UndoDeprecate</td>
<td>no</td>
<td>Whether to undeprecate a deprecated thing type. If true, the thing type will not be deprecated anymore and you can associate it with things.</td>
</tr>
</tbody>
</table>

**Errors:**

- **InternalException**
  - An unexpected error has occurred.

- **InvalidRequestException**
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ServiceUnavailableException**
  - The service is temporarily unavailable.
ResourceNotFoundException
  The specified resource does not exist.
  HTTP response code: 404

InvalidRequestException
  The contents of the request were invalid. For example, this code is returned when an
  UpdateJobExecution request contains invalid status details. The message contains details about the
  error.
  HTTP response code: 400

ThrottlingException
  The rate exceeds the limit.
  HTTP response code: 429

UnauthorizedException
  You are not authorized to perform this operation.
  HTTP response code: 401

ServiceUnavailableException
  The service is temporarily unavailable.
  HTTP response code: 503

InternalFailureException
  An unexpected error has occurred.
  HTTP response code: 500

**cli**

**Synopsis:**

```
aws iot deprecate-thing-type \
  --thing-type-name <value> \
  [--undo-deprecate | --no-undo-deprecate] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

**cli-input-json format:**

```
{
  "thingTypeName": "string",
  "undoDeprecate": "boolean"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>string</td>
<td>The name of the thing type to deprecate.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td>pattern: [a-zA-Z0-9_:-]+</td>
</tr>
</tbody>
</table>
DescribeAccountAuditConfiguration

Gets information about the Device Defender audit settings for this account. Settings include how audit notifications are sent and which audit checks are enabled or disabled.

https

Request syntax:

GET /audit/configuration

Response syntax:

Content-type: application/json
{
    "roleArn": "string",
}
"auditNotificationTargetConfigurations": {
    "string": {
        "targetArn": "string",
        "roleArn": "string",
        "enabled": "boolean"
    }
},
"auditCheckConfigurations": {
    "string": {
        "enabled": "boolean"
    }
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>RoleArn</td>
<td>no</td>
<td>The ARN of the role that grants permission to AWS IoT to access information about your devices, policies, certificates and other items as necessary when performing an audit. On the first call to UpdateAccountAuditConfiguration this parameter is required.</td>
</tr>
<tr>
<td>auditNotificationTargetConfigurations</td>
<td>AuditNotificationTargetConfigurations</td>
<td>no</td>
<td>Information about the targets to which audit notifications are sent for this account.</td>
</tr>
<tr>
<td>auditCheckConfigurations</td>
<td>AuditCheckConfigurations</td>
<td>no</td>
<td>Which audit checks are enabled and disabled for this account.</td>
</tr>
</tbody>
</table>

Errors:

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:
### cli-input-json format:

```json
{}
```

### Output:

```json
{
  "roleArn": "string",
  "auditNotificationTargetConfigurations": {
    "string": {
      "targetArn": "string",
      "roleArn": "string",
      "enabled": "boolean"
    }
  },
  "auditCheckConfigurations": {
    "String": {
      "enabled": "boolean"
    }
  }
}
```

### cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants permission to AWS IoT to access information about your devices, policies, certificates and other items as necessary when performing an audit. On the first call to UpdateAccountAuditConfiguration this parameter is required.</td>
</tr>
<tr>
<td></td>
<td>length- max:2048 min:20</td>
<td></td>
</tr>
<tr>
<td>auditNotificationTargetConfigurations</td>
<td>map</td>
<td>Information about the targets to which audit notifications are sent for this account.</td>
</tr>
<tr>
<td>targetArn</td>
<td>string</td>
<td>The ARN of the target (SNS topic) to which audit notifications are sent.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants permission to send notifications to the target.</td>
</tr>
<tr>
<td></td>
<td>length- max:2048 min:20</td>
<td></td>
</tr>
<tr>
<td>enabled</td>
<td>boolean</td>
<td>True if notifications to the target are enabled.</td>
</tr>
<tr>
<td>auditCheckConfigurations</td>
<td>map</td>
<td>Which audit checks are enabled and disabled for this account.</td>
</tr>
</tbody>
</table>
DescribeAuditTask

Gets information about a Device Defender audit.

**https**

**Request syntax:**

```plaintext
GET /audit/tasks/taskId
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>AuditTaskId</td>
<td>yes</td>
<td>The ID of the audit whose information you want to get.</td>
</tr>
</tbody>
</table>

**Response syntax:**

```json
Content-type: application/json

{
  "taskStatus": "string",
  "taskType": "string",
  "taskStartTime": "timestamp",
  "taskStatistics": {
    "totalChecks": "integer",
    "inProgressChecks": "integer",
    "waitingForDataCollectionChecks": "integer",
    "compliantChecks": "integer",
    "nonCompliantChecks": "integer",
    "failedChecks": "integer",
    "canceledChecks": "integer"
  },
  "scheduledAuditName": "string",
  "auditDetails": {
    "string": {
      "string": {
      }
    }
  }
}```
"checkRunStatus": "string",
"checkCompliant": "boolean",
"totalResourcesCount": "long",
"nonCompliantResourcesCount": "long",
"errorCode": "string",
"message": "string"
}

}  

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskStatus</td>
<td>AuditTaskStatus</td>
<td>no</td>
<td>The status of the audit: one of &quot;IN_PROGRESS&quot;, &quot;COMPLETED&quot;, &quot;FAILED&quot;, or &quot;CANCELED&quot;.</td>
</tr>
<tr>
<td>taskType</td>
<td>AuditTaskType</td>
<td>no</td>
<td>The type of audit: &quot;ON_DEMAND_AUDIT_TASK&quot; or &quot;SCHEDULED_AUDIT_TASK&quot;.</td>
</tr>
<tr>
<td>taskStartTime</td>
<td>Timestamp</td>
<td>no</td>
<td>The time the audit started.</td>
</tr>
<tr>
<td>taskStatistics</td>
<td>TaskStatistics</td>
<td>no</td>
<td>Statistical information about the audit.</td>
</tr>
<tr>
<td>scheduledAuditName</td>
<td>ScheduledAuditName</td>
<td>no</td>
<td>The name of the scheduled audit (only if the audit was a scheduled audit).</td>
</tr>
<tr>
<td>auditDetails</td>
<td>AuditDetails</td>
<td>no</td>
<td>Detailed information about each check performed during this audit.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.
HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot describe-audit-task \
  --task-id <value> \ 
  [--cli-input-json <value>] \ 
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "taskId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>string</td>
<td>The ID of the audit whose information you want to get.</td>
</tr>
<tr>
<td>length- max:40 min:1</td>
<td>pattern: [a-zA-Z0-9-]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```
{
  "taskStatus": "string",
  "taskType": "string",
  "taskStartTime": "timestamp",
  "taskStatistics": {
    "totalChecks": "integer",
    "inProgressChecks": "integer",
    "waitingForDataCollectionChecks": "integer",
    "compliantChecks": "integer",
    "nonCompliantChecks": "integer",
    "failedChecks": "integer",
    "canceledChecks": "integer"
  },
  "scheduledAuditName": "string",
  "auditDetails": {
    "string": {
      "checkRunStatus": "string",
      "checkCompliant": "boolean",
      "totalResourcesCount": "long",
      "nonCompliantResourcesCount": "long",
      "errorCode": "string",
      "message": "string"
    }
  }
}
```
### cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskStatus</td>
<td>string</td>
<td>The status of the audit: one of &quot;IN_PROGRESS&quot;, &quot;COMPLETED&quot;, &quot;FAILED&quot;, or &quot;CANCELED&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>enum</strong>: IN_PROGRESS</td>
</tr>
<tr>
<td>taskType</td>
<td>string</td>
<td>The type of audit: &quot;ON_DEMAND_AUDIT_TASK&quot; or &quot;SCHEDULED_AUDIT_TASK&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>enum</strong>: ON_DEMAND_AUDIT_TASK</td>
</tr>
<tr>
<td>taskStartTime</td>
<td>timestamp</td>
<td>The time the audit started.</td>
</tr>
<tr>
<td>taskStatistics</td>
<td>TaskStatistics</td>
<td>Statistical information about the audit.</td>
</tr>
<tr>
<td>totalChecks</td>
<td>integer</td>
<td>The number of checks in this audit.</td>
</tr>
<tr>
<td>inProgressChecks</td>
<td>integer</td>
<td>The number of checks in progress.</td>
</tr>
<tr>
<td>waitingForDataCollectionChecks</td>
<td>integer</td>
<td>The number of checks waiting for data collection.</td>
</tr>
<tr>
<td>compliantChecks</td>
<td>integer</td>
<td>The number of checks that found compliant resources.</td>
</tr>
<tr>
<td>nonCompliantChecks</td>
<td>integer</td>
<td>The number of checks that found non-compliant resources.</td>
</tr>
<tr>
<td>failedChecks</td>
<td>integer</td>
<td>The number of checks</td>
</tr>
<tr>
<td>canceledChecks</td>
<td>integer</td>
<td>The number of checks that did not run because the audit was canceled.</td>
</tr>
<tr>
<td>scheduledAuditName</td>
<td>string</td>
<td>The name of the scheduled audit (only if the audit was a scheduled audit).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>length- max:128 min:1</strong></td>
</tr>
<tr>
<td>auditDetails</td>
<td>map</td>
<td>Detailed information about each check performed during this audit.</td>
</tr>
<tr>
<td>checkRunStatus</td>
<td>string</td>
<td>The completion status of this check, one of &quot;IN_PROGRESS&quot;,</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name</td>
<td></td>
<td>&quot;WAITING_FOR_DATA_COLLECTION&quot;, &quot;CANCELED&quot;, &quot;COMPLETED_COMPLIANT&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;COMPLETED_NON_COMPLIANT&quot;, or &quot;FAILED&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: IN_PROGRESS</td>
</tr>
<tr>
<td>checkCompliant</td>
<td>boolean</td>
<td>True if the check completed and found all resources compliant.</td>
</tr>
<tr>
<td>totalResourcesCount</td>
<td>long</td>
<td>The number of resources on which the check was performed.</td>
</tr>
<tr>
<td>nonCompliantResourcesCount</td>
<td>long</td>
<td>The number of resources that the check found non-compliant.</td>
</tr>
<tr>
<td>errorCode</td>
<td>string</td>
<td>The code of any error encountered when performing this check during this</td>
</tr>
<tr>
<td></td>
<td></td>
<td>audit. One of &quot;INSUFFICIENT_PERMISSIONS&quot;, or &quot;AUDIT_CHECK_DISABLED&quot;.</td>
</tr>
<tr>
<td>message</td>
<td>string</td>
<td>The message associated with any error encountered when performing this check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>length- max:2048 The message associated with this audit.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceNotFoundException

The specified resource does not exist.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

DescribeAuthorizer

Describes an authorizer.
https

Request syntax:

GET /authorizer/authorizerName

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>AuthorizerName</td>
<td>yes</td>
<td>The name of the authorizer to describe.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```json
{
  "authorizerDescription": {
    "authorizerName": "string",
    "authorizerArn": "string",
    "authorizerFunctionArn": "string",
    "tokenKeyName": "string",
    "tokenSigningPublicKeys": {
      "string": "string"
    },
    "status": "string",
    "creationDate": "timestamp",
    "lastModifiedDate": "timestamp"
  }
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerDescription</td>
<td>AuthorizerDescription</td>
<td>no</td>
<td>The authorizer description.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.
HTTP response code: 429
UnauthorizedException
You are not authorized to perform this operation.

HTTP response code: 401
ServiceUnavailableException
The service is temporarily unavailable.

HTTP response code: 503
InternalFailureException
An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```bash
aws iot describe-authorizer \
--authorizer-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "authorizerName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>string</td>
<td>The name of the authorizer to describe.</td>
</tr>
<tr>
<td>length- max:128</td>
<td>min:1</td>
<td></td>
</tr>
<tr>
<td>pattern: [w=,-@]+</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
  "authorizerDescription": {
    "authorizerName": "string",
    "authorizerArn": "string",
    "authorizerFunctionArn": "string",
    "tokenKeyName": "string",
    "tokenSigningPublicKeys": {
      "string": "string"
    },
    "status": "string",
    "creationDate": "timestamp",
    "lastModifiedDate": "timestamp"
  }
}
```
cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerDescription</td>
<td>AuthorizerDescription</td>
<td>The authorizer description.</td>
</tr>
<tr>
<td>authorizerName</td>
<td>string</td>
<td>The authorizer name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w=,@-]+</td>
<td></td>
</tr>
<tr>
<td>authorizerArn</td>
<td>string</td>
<td>The authorizer ARN.</td>
</tr>
<tr>
<td>authorizerFunctionArn</td>
<td>string</td>
<td>The authorizer's Lambda function ARN.</td>
</tr>
<tr>
<td>tokenKeyName</td>
<td>string</td>
<td>The key used to extract the token from the HTTP headers.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-]+</td>
<td></td>
</tr>
<tr>
<td>tokenSigningPublicKeys</td>
<td>map</td>
<td>The public keys used to validate the token signature returned by your</td>
</tr>
<tr>
<td></td>
<td></td>
<td>custom authentication service.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the authorizer.</td>
</tr>
<tr>
<td></td>
<td>enum: ACTIVE</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The UNIX timestamp of when the authorizer was created.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>timestamp</td>
<td>The UNIX timestamp of when the authorizer was last updated.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException
The specified resource does not exist.

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException
The rate exceeds the limit.

UnauthorizedException
You are not authorized to perform this operation.

ServiceUnavailableException
The service is temporarily unavailable.

InternalFailureException
An unexpected error has occurred.
DescribeCACertificate

Describes a registered CA certificate.

https

Request syntax:

GET /cacertificate/caCertificateId

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>CertificateId</td>
<td>yes</td>
<td>The CA certificate identifier.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```
{
  "certificateDescription": {
    "certificateArn": "string",
    "certificateId": "string",
    "status": "string",
    "certificatePem": "string",
    "ownedBy": "string",
    "creationDate": "timestamp",
    "autoRegistrationStatus": "string",
    "lastModifiedDate": "timestamp",
    "customerVersion": "integer",
    "generationId": "string",
    "validity": {
      "notBefore": "timestamp",
      "notAfter": "timestamp"
    }
  },
  "registrationConfig": {
    "templateBody": "string",
    "roleArn": "string"
  }
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateDescription</td>
<td>CACertificateDescription</td>
<td>no</td>
<td>The CA certificate description.</td>
</tr>
<tr>
<td>registrationConfig</td>
<td>RegistrationConfig</td>
<td>no</td>
<td>Information about the registration configuration.</td>
</tr>
</tbody>
</table>

Errors:
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

cli

Synopsis:

```
aws iot describe-ca-certificate \
  --certificate-id <value> \ 
  [--cli-input-json <value>] \ 
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "certificateId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>string</td>
<td>The CA certificate identifier.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>length- max:64 min:64</td>
<td>pattern: (0x)?[a-fA-F0-9]+</td>
<td></td>
</tr>
<tr>
<td>certificateDescription</td>
<td>CACertificateDescription</td>
<td>The CA certificate description.</td>
</tr>
<tr>
<td>certificateArn</td>
<td>string</td>
<td>The CA certificate ARN.</td>
</tr>
<tr>
<td>certificateId</td>
<td>string</td>
<td>The CA certificate ID.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of a CA certificate.</td>
</tr>
<tr>
<td>certificatePem</td>
<td>string</td>
<td>The CA certificate data, in PEM format.</td>
</tr>
<tr>
<td>ownedBy</td>
<td>string</td>
<td>The owner of the CA certificate.</td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The date the CA certificate was created.</td>
</tr>
</tbody>
</table>
## DescribeCACertificate

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoRegistrationStatus</td>
<td>string</td>
<td>Whether the CA certificate configured for auto registration of device certificates. Valid values are &quot;ENABLE&quot; and &quot;DISABLE&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: ENABLE</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>timestamp</td>
<td>The date the CA certificate was last modified.</td>
</tr>
<tr>
<td>customerVersion</td>
<td>integer</td>
<td>The customer version of the CA certificate.</td>
</tr>
<tr>
<td></td>
<td>range- min:1</td>
<td></td>
</tr>
<tr>
<td>generationId</td>
<td>string</td>
<td>The generation ID of the CA certificate.</td>
</tr>
<tr>
<td>validity</td>
<td>CertificateValidity</td>
<td>When the CA certificate is valid.</td>
</tr>
<tr>
<td>notBefore</td>
<td>timestamp</td>
<td>The certificate is not valid before this date.</td>
</tr>
<tr>
<td>notAfter</td>
<td>timestamp</td>
<td>The certificate is not valid after this date.</td>
</tr>
<tr>
<td>registrationConfig</td>
<td>RegistrationConfig</td>
<td>Information about the registration configuration.</td>
</tr>
<tr>
<td>templateBody</td>
<td>string</td>
<td>The template body.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role.</td>
</tr>
<tr>
<td></td>
<td>length-    max:2048 min:20</td>
<td></td>
</tr>
</tbody>
</table>

### Errors:

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ThrottlingException**
  
  The rate exceeds the limit.

- **UnauthorizedException**
  
  You are not authorized to perform this operation.

- **ServiceUnavailableException**
  
  The service is temporarily unavailable.

- **InternalFailureException**
  
  An unexpected error has occurred.

- **ResourceNotFoundException**
  
  The specified resource does not exist.
DescribeCertificate

Gets information about the specified certificate.

https

Request syntax:

GET /certificates/certificateId

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>CertificateId</td>
<td>yes</td>
<td>The ID of the certificate. (The last part of the certificate ARN contains the certificate ID.)</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```
{
  "certificateDescription": {
    "certificateArn": "string",
    "certificateId": "string",
    "caCertificateId": "string",
    "status": "string",
    "certificatePem": "string",
    "ownedBy": "string",
    "previousOwnedBy": "string",
    "creationDate": "timestamp",
    "lastModifiedDate": "timestamp",
    "customerVersion": "integer",
    "transferData": {
      "transferMessage": "string",
      "rejectReason": "string",
      "transferDate": "timestamp",
      "acceptDate": "timestamp",
      "rejectDate": "timestamp"
    },
    "generationId": "string",
    "validity": {
      "notBefore": "timestamp",
      "notAfter": "timestamp"
    }
  }
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateDescription</td>
<td>CertificateDescription</td>
<td>no</td>
<td>The description of the certificate.</td>
</tr>
</tbody>
</table>
Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

cli

Synopsis:

```
aws iot describe-certificate \
  --certificate-id <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "certificateId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>string</td>
<td>The ID of the certificate. (The last part of the certificate ARN contains the certificate ID.)</td>
</tr>
</tbody>
</table>
Output:

```
{
  "certificateDescription": {
    "certificateArn": "string",
    "certificateId": "string",
    "caCertificateId": "string",
    "status": "string",
    "certificatePem": "string",
    "ownedBy": "string",
    "previousOwnedBy": "string",
    "creationDate": "timestamp",
    "lastModifiedDate": "timestamp",
    "customerVersion": "integer",
    "transferData": {
      "transferMessage": "string",
      "rejectReason": "string",
      "transferDate": "timestamp",
      "acceptDate": "timestamp",
      "rejectDate": "timestamp"
    },
    "generationId": "string",
    "validity": {
      "notBefore": "timestamp",
      "notAfter": "timestamp"
    }
  }
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateDescription</td>
<td>CertificateDescription</td>
<td>The description of the certificate.</td>
</tr>
<tr>
<td>certificateArn</td>
<td>string</td>
<td>The ARN of the certificate.</td>
</tr>
<tr>
<td>certificateId</td>
<td>string</td>
<td>The ID of the certificate.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: (0x)?[a-fA-F0-9]+</td>
<td></td>
</tr>
<tr>
<td>caCertificateId</td>
<td>string</td>
<td>The certificate ID of the CA certificate used to sign this certificate.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: (0x)?[a-fA-F0-9]+</td>
<td></td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the certificate.</td>
</tr>
<tr>
<td></td>
<td>enum: ACTIVE</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>certificatePem</td>
<td>string</td>
<td>The certificate data, in PEM format.</td>
</tr>
<tr>
<td></td>
<td>length- max:65536 min:1</td>
<td></td>
</tr>
<tr>
<td>ownedBy</td>
<td>string</td>
<td>The ID of the AWS account that owns the certificate.</td>
</tr>
</tbody>
</table>
### DescribeCertificate

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>length- max:12 min:12</td>
<td></td>
</tr>
<tr>
<td>previousOwnedBy</td>
<td>string</td>
<td>The ID of the AWS account of the previous owner of the certificate.</td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The date and time the certificate was created.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>timestamp</td>
<td>The date and time the certificate was last modified.</td>
</tr>
<tr>
<td>customerVersion</td>
<td>integer range- min:1</td>
<td>The customer version of the certificate.</td>
</tr>
<tr>
<td>transferData</td>
<td>TransferData</td>
<td>The transfer data.</td>
</tr>
<tr>
<td>transferMessage</td>
<td>string</td>
<td>The transfer message.</td>
</tr>
<tr>
<td>rejectReason</td>
<td>string</td>
<td>The reason why the transfer was rejected.</td>
</tr>
<tr>
<td>transferDate</td>
<td>timestamp</td>
<td>The date the transfer took place.</td>
</tr>
<tr>
<td>acceptDate</td>
<td>timestamp</td>
<td>The date the transfer was accepted.</td>
</tr>
<tr>
<td>rejectDate</td>
<td>timestamp</td>
<td>The date the transfer was rejected.</td>
</tr>
<tr>
<td>generationId</td>
<td>string</td>
<td>The generation ID of the certificate.</td>
</tr>
<tr>
<td>validity</td>
<td>CertificateValidity</td>
<td>When the certificate is valid.</td>
</tr>
<tr>
<td>notBefore</td>
<td>timestamp</td>
<td>The certificate is not valid before this date.</td>
</tr>
<tr>
<td>notAfter</td>
<td>timestamp</td>
<td>The certificate is not valid after this date.</td>
</tr>
</tbody>
</table>

### Errors:

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

**ThrottlingException**

The rate exceeds the limit.
UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

ResourceNotFoundException

The specified resource does not exist.

DescribeDefaultAuthorizer

Describes the default authorizer.

https

Request syntax:

GET /default-authorizer

Response syntax:

Content-type: application/json

```
{
    "authorizerDescription": {
        "authorizerName": "string",
        "authorizerArn": "string",
        "authorizerFunctionArn": "string",
        "tokenKeyName": "string",
        "tokenSigningPublicKeys": {
            "string": "string"
        },
        "status": "string",
        "creationDate": "timestamp",
        "lastModifiedDetail": "timestamp"
    }
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerDescription</td>
<td>AuthorizerDescription</td>
<td>no</td>
<td>The default authorizer's description.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException

The specified resource does not exist.
HTTP response code: 404
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400
ThrottlingException

The rate exceeds the limit.

HTTP response code: 429
UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401
ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503
InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

aws iot describe-default-authorizer  
[--cli-input-json <value>] 
[--generate-cli-skeleton]

cli-input-json format:

{
}

Output:

{
  "authorizerDescription": {
    "authorizerName": "string",
    "authorizerArn": "string",
    "authorizerFunctionArn": "string",
    "tokenKeyName": "string",
    "tokenSigningPublicKeys": {
      "string": "string"
    },
    "status": "string",
    "creationDate": "timestamp",
  }
}
DescribeDefaultAuthorizer

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerDescription</td>
<td>AuthorizerDescription</td>
<td>The default authorizer's description.</td>
</tr>
<tr>
<td>authorizerName</td>
<td>string</td>
<td>The authorizer name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w=,@-]+</td>
<td></td>
</tr>
<tr>
<td>authorizerArn</td>
<td>string</td>
<td>The authorizer ARN.</td>
</tr>
<tr>
<td>authorizerFunctionArn</td>
<td>string</td>
<td>The authorizer's Lambda function ARN.</td>
</tr>
<tr>
<td>tokenKeyName</td>
<td>string</td>
<td>The key used to extract the token from the HTTP headers.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-]+</td>
<td></td>
</tr>
<tr>
<td>tokenSigningPublicKeys</td>
<td>map</td>
<td>The public keys used to validate the token signature returned by your custom authentication service.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the authorizer.</td>
</tr>
<tr>
<td></td>
<td>enum: ACTIVE</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The UNIX timestamp of when the authorizer was created.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>timestamp</td>
<td>The UNIX timestamp of when the authorizer was last updated.</td>
</tr>
</tbody>
</table>

Errors:

- **ResourceNotFoundException**
  - The specified resource does not exist.

- **InvalidRequestException**
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ThrottlingException**
  - The rate exceeds the limit.

- **UnauthorizedException**
  - You are not authorized to perform this operation.
DescribeEndpoint

Returns a unique endpoint specific to the AWS account making the call.

https

Request syntax:

GET /endpoint?endpointType=endpointType

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpointType</td>
<td>EndpointType</td>
<td>no</td>
<td>The endpoint type (such as iot:Data, iot:CredentialProvider, and iot:Jobs).</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{  "endpointAddress": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpointAddress</td>
<td>EndpointAddress</td>
<td>no</td>
<td>The endpoint. The format of the endpoint is as follows: identifier.iot.region.amazonaws.com.</td>
</tr>
</tbody>
</table>

Errors:

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

cli

Synopsis:

```
aws iot describe-endpoint \
    [--endpoint-type <value>] \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

cli-input-json format:

```
{
    "endpointType": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpointType</td>
<td>string</td>
<td>The endpoint type (such as iot:Data, iot:CredentialProvider, and iot:Jobs).</td>
</tr>
</tbody>
</table>

Output:

```
{
    "endpointAddress": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpointAddress</td>
<td>string</td>
<td>The endpoint. The format of the endpoint is as follows: identifier.iot.region.amazonaws.com.</td>
</tr>
</tbody>
</table>
Errors:

InternalFailureException

An unexpected error has occurred.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

UnauthorizedException

You are not authorized to perform this operation.

ThrottlingException

The rate exceeds the limit.

DescribeEventConfigurations

Describes event configurations.

https

Request syntax:

GET /event-configurations

Response syntax:

Content-type: application/json

```json
{
    "eventConfigurations": {
        "string": {
            "Enabled": "boolean"
        }
    },
    "creationDate": "timestamp",
    "lastModifiedDate": "timestamp"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventConfigurations</td>
<td>EventConfigurations</td>
<td>no</td>
<td>The event configurations.</td>
</tr>
<tr>
<td>creationDate</td>
<td>CreationDate</td>
<td>no</td>
<td>The creation date of the event configuration.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>LastModifiedDate</td>
<td>no</td>
<td>The date the event configurations were last modified.</td>
</tr>
</tbody>
</table>
Errors:

InternalFailureException

An unexpected error has occurred.
HTTP response code: 500

ThrottlingException

The rate exceeds the limit.
HTTP response code: 429

cli

Synopsis:

```
aws iot describe-event-configurations \ 
    [--cli-input-json <value>] \ 
    [--generate-cli-skeleton]
```

cli-input-json format:

```
{
}
```

Output:

```
{
    "eventConfigurations": {
        "string": {
            "Enabled": "boolean"
        },
        "creationDate": "timestamp",
        "lastModifiedDate": "timestamp"
    }
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventConfigurations</td>
<td>map</td>
<td>The event configurations.</td>
</tr>
<tr>
<td>Enabled</td>
<td>boolean</td>
<td>True to enable the configuration.</td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The creation date of the event configuration.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>timestamp</td>
<td>The date the event configurations were last modified.</td>
</tr>
</tbody>
</table>

Errors:

InternalFailureException

An unexpected error has occurred.
ThrottlingException

The rate exceeds the limit.

DescribeIndex

Describes a search index.

https

Request syntax:

```
GET /indices/indexName
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>indexName</td>
<td>IndexName</td>
<td>yes</td>
<td>The index name.</td>
</tr>
</tbody>
</table>

Response syntax:

```
Content-type: application/json

{
    "indexName": "string",
    "indexStatus": "string",
    "schema": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>indexName</td>
<td>IndexName</td>
<td>no</td>
<td>The index name.</td>
</tr>
<tr>
<td>indexStatus</td>
<td>IndexStatus</td>
<td>no</td>
<td>The index status.</td>
</tr>
<tr>
<td>schema</td>
<td>IndexSchema</td>
<td>no</td>
<td>Contains a value that specifies the type of indexing performed. Valid values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1. REGISTRY – Your thing index will contain only registry data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. REGISTRY_AND_SHADOW - Your thing index will contain registry and shadow data.</td>
</tr>
</tbody>
</table>

Errors:

754
**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**UnauthorizedException**

You are not authorized to perform this operation.

HTTP response code: 401

**ServiceUnavailableException**

The service is temporarily unavailable.

HTTP response code: 503

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404

---

**cli**

**Synopsis:**

```bash
aws iot describe-index \
  --index-name <value> \ 
  [--cli-input-json <value>] \ 
  [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
  "indexName": "string"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>indexName</td>
<td>string</td>
<td>The index name.</td>
</tr>
<tr>
<td></td>
<td>length-</td>
<td>max:128 min:1</td>
</tr>
</tbody>
</table>
DescribeIndex

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>indexName</td>
<td>string</td>
<td>The index name.</td>
</tr>
<tr>
<td>indexStatus</td>
<td>string</td>
<td>The index status. enum: ACTIVE</td>
</tr>
<tr>
<td>schema</td>
<td>string</td>
<td>Contains a value that specifies the type of indexing performed. Valid values are: 1. REGISTRY – Your thing index will contain only registry data. 2. REGISTRY_AND_SHADOW - Your thing index will contain registry and shadow data.</td>
</tr>
</tbody>
</table>

Output:

```json
{
  "indexName": "string",
  "indexStatus": "string",
  "schema": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>indexName</td>
<td>string</td>
<td>The index name.</td>
</tr>
<tr>
<td>indexStatus</td>
<td>string</td>
<td>The index status. enum: ACTIVE</td>
</tr>
<tr>
<td>schema</td>
<td>string</td>
<td>Contains a value that specifies the type of indexing performed. Valid values are: 1. REGISTRY – Your thing index will contain only registry data. 2. REGISTRY_AND_SHADOW - Your thing index will contain registry and shadow data.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.
ResourceNotFoundException

The specified resource does not exist.

DescribeJob

Describes a job.

https

Request syntax:

GET /jobs/jobId

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>JobId</td>
<td>yes</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```json
{
    "documentSource": "string",
    "job": {
        "jobArn": "string",
        "jobId": "string",
        "targetSelection": "string",
        "status": "string",
        "forceCanceled": "boolean",
        "comment": "string",
        "targets": [
            "string"
        ],
        "description": "string",
        "presignedUrlConfig": {
            "roleArn": "string",
            "expiresInSec": "long"
        },
    },
    "jobExecutionsRolloutConfig": {
        "maximumPerMinute": "integer"
    },
    "createdAt": "timestamp",
    "lastUpdatedAt": "timestamp",
    "completedAt": "timestamp",
    "jobProcessDetails": {
        "processingTargets": [
            "string"
        ],
        "numberOfCanceledThings": "integer",
        "numberOfSucceededThings": "integer",
        "numberOfFailedThings": "integer"
    }
}
```
"numberOfRejectedThings": "integer",
"numberOfQueuedThings": "integer",
"numberOfInProgressThings": "integer",
"numberOfRemovedThings": "integer"
}
}
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>documentSource</td>
<td>JobDocumentSource</td>
<td>no</td>
<td>An S3 link to the job document.</td>
</tr>
<tr>
<td>job</td>
<td>Job</td>
<td>no</td>
<td>Information about the job.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

cli

Synopsis:

aws iot describe-job \
  --job-id <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]

cli-input-json format:

{
  "jobId": "string"
DescribeJob

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobld</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
</tbody>
</table>

Output:

```json
{
    "documentSource": "string",
    "job": {
        "jobArn": "string",
        "jobId": "string",
        "targetSelection": "string",
        "status": "string",
        "forceCanceled": "boolean",
        "comment": "string",
        "targets": [
            "string"
        ],
        "description": "string",
        "presignedUrlConfig": {
            "roleArn": "string",
            "expiresInSec": "long"
        },
        "jobExecutionsRolloutConfig": {
            "maximumPerMinute": "integer"
        },
        "createdAt": "timestamp",
        "lastUpdatedAt": "timestamp",
        "completedAt": "timestamp",
        "jobProcessDetails": {
            "processingTargets": [
                "string"
            ],
            "numberOfCanceledThings": "integer",
            "numberOfSucceededThings": "integer",
            "numberOfFailedThings": "integer",
            "numberOfRejectedThings": "integer",
            "numberOfQueuedThings": "integer",
            "numberOfInProgressThings": "integer",
            "numberOfRemovedThings": "integer"
        }
    }
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>documentSource</td>
<td>string</td>
<td>An S3 link to the job document.</td>
</tr>
<tr>
<td>job</td>
<td>Job</td>
<td>Information about the job.</td>
</tr>
</tbody>
</table>

759
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobArn</td>
<td>string</td>
<td>An ARN identifying the job with format &quot;arn:aws:iot:region:account:job/jobId&quot;.</td>
</tr>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:1 pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>targetSelection</td>
<td>string</td>
<td>Specifies whether the job will continue to run (CONTINUOUS), or will be complete after all those things specified as targets have completed the job (SNAPSHOT). If continuous, the job may also be run on a thing when a change is detected in a target. For example, a job will run on a device when the thing representing the device is added to a target group, even after the job was completed by all things originally in the group.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the job, one of IN_PROGRESS, CANCELED, or COMPLETED.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: IN_PROGRESS</td>
</tr>
<tr>
<td>forceCanceled</td>
<td>boolean</td>
<td>Will be true if the job was canceled with the optional force parameter set to true.</td>
</tr>
<tr>
<td>comment</td>
<td>string</td>
<td>If the job was updated, describes the reason for the update.</td>
</tr>
<tr>
<td></td>
<td>length- max:2028 pattern: [^\p{C}]+</td>
<td></td>
</tr>
<tr>
<td>targets</td>
<td>list</td>
<td>A list of IoT things and thing groups to which the job should be sent.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>A short text description of the job.</td>
</tr>
<tr>
<td></td>
<td>length- max:2028 pattern: [^\p{C}]+</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>presignedUrlConfig</td>
<td>PresignedUrlConfig</td>
<td>Configuration for pre-signed S3 URLs.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of an IAM role that grants permission to download files from the S3 bucket where the job data/updates are stored. The role must also grant permission for IoT to download the files.</td>
</tr>
<tr>
<td>expiresInSec</td>
<td>long</td>
<td>How long (in seconds) pre-signed URLs are valid. Valid values are 60 - 3600, the default value is 3600 seconds. Pre-signed URLs are generated when Jobs receives an MQTT request for the job document.</td>
</tr>
<tr>
<td>jobExecutionsRolloutConfig</td>
<td>JobExecutionsRolloutConfig</td>
<td>Allows you to create a staged rollout of a job.</td>
</tr>
<tr>
<td>maximumPerMinute</td>
<td>integer</td>
<td>The maximum number of things that will be notified of a pending job, per minute. This parameter allows you to create a staged rollout.</td>
</tr>
<tr>
<td>createdAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job was created.</td>
</tr>
<tr>
<td>lastUpdatedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job was last updated.</td>
</tr>
<tr>
<td>completedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job was completed.</td>
</tr>
<tr>
<td>jobProcessDetails</td>
<td>JobProcessDetails</td>
<td>Details about the job process.</td>
</tr>
<tr>
<td>processingTargets</td>
<td>list</td>
<td>The target devices to which the job execution is being rolled out. This value will be null after the job execution has finished rolling out to all the target devices.</td>
</tr>
<tr>
<td>numberOfCanceledThings</td>
<td>integer</td>
<td>The number of things that cancelled the job.</td>
</tr>
<tr>
<td>numberOfSucceededThings</td>
<td>integer</td>
<td>The number of things which successfully completed the job.</td>
</tr>
<tr>
<td>numberOfFailedThings</td>
<td>integer</td>
<td>The number of things that failed executing the job.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>numberOfRejectedThings</td>
<td>integer</td>
<td>The number of things that rejected the job.</td>
</tr>
<tr>
<td>numberOfQueuedThings</td>
<td>integer</td>
<td>The number of things that are awaiting execution of the job.</td>
</tr>
<tr>
<td>numberOfInProgressThings</td>
<td>integer</td>
<td>The number of things currently executing the job.</td>
</tr>
<tr>
<td>numberOfRemovedThings</td>
<td>integer</td>
<td>The number of things that are no longer scheduled to execute the job because they have been deleted or have been removed from the group that was a target of the job.</td>
</tr>
</tbody>
</table>

**Errors:**

- **InvalidRequestException**
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ResourceNotFoundException**
  The specified resource does not exist.

- **ThrottlingException**
  The rate exceeds the limit.

- **ServiceUnavailableException**
  The service is temporarily unavailable.

**DescribeJobExecution**

Describes a job execution.

**https**

**Request syntax:**

```
GET /things/thingName/jobs/jobId?executionNumber=executionNumber
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>JobId</td>
<td>yes</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
</tbody>
</table>
## AWS IoT Developer Guide

### DescribeJobExecution

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing on which the job execution is running.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>ExecutionNumber</td>
<td>no</td>
<td>A string (consisting of the digits &quot;0&quot; through &quot;9&quot; which is used to specify a particular job execution on a particular device.</td>
</tr>
</tbody>
</table>

#### Response syntax:

Content-type: application/json

```json
{
  "execution": {
    "jobId": "string",
    "status": "string",
    "forceCanceled": "boolean",
    "statusDetails": {
      "detailsMap": {
        "string": "string"
      }
    },
    "thingArn": "string",
    "queuedAt": "timestamp",
    "startedAt": "timestamp",
    "lastUpdatedAt": "timestamp",
    "executionNumber": "long",
    "versionNumber": "long"
  }
}
```

#### Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>execution</td>
<td>JobExecution</td>
<td>no</td>
<td>Information about the job execution.</td>
</tr>
</tbody>
</table>

#### Errors:

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404
ThrottlingException

The rate exceeds the limit.
HTTP response code: 429

ServiceUnavailableException

The service is temporarily unavailable.
HTTP response code: 503

cli

Synopsis:

```
aws iot describe-job-execution \
  --job-id <value> \
  --thing-name <value> \
  [--execution-number <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "jobId": "string",
  "thingName": "string",
  "executionNumber": "long"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>length- max:64 min:1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pattern: [a-zA-Z0-9_-]+</td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing on which the job execution is running.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>length- max:128 min:1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pattern: [a-zA-Z0-9_-]+</td>
</tr>
<tr>
<td>executionNumber</td>
<td>long</td>
<td>A string (consisting of the digits &quot;0&quot; through &quot;9&quot;) which is used to specify a particular job execution on a particular device.</td>
</tr>
</tbody>
</table>

Output:

```
{
  "execution": {
    "jobId": "string",
    "status": "string",
```

764
"forceCanceled": "boolean",
"statusDetails": {
  "detailsMap": {
    "string": "string"
  }
},
"thingArn": "string",
"queuedAt": "timestamp",
"startedAt": "timestamp",
"lastUpdatedAt": "timestamp",
"executionNumber": "long",
"versionNumber": "long"

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>execution</td>
<td>JobExecution</td>
<td>Information about the job execution.</td>
</tr>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to the job when it was created.</td>
</tr>
<tr>
<td>length- max:64 min:1 pattern: [a-zA-Z0-9_.-]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the job execution (IN_PROGRESS, QUEUED, FAILED, SUCCESS, CANCELED, or REJECTED).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: QUEUED</td>
</tr>
<tr>
<td>forceCanceled</td>
<td>boolean</td>
<td>Will be true if the job execution was canceled with the optional force parameter set to true.</td>
</tr>
<tr>
<td>statusDetails</td>
<td>JobExecutionStatusDetails</td>
<td>A collection of name/value pairs that describe the status of the job execution.</td>
</tr>
<tr>
<td>detailsMap</td>
<td>map</td>
<td>The job execution status.</td>
</tr>
<tr>
<td>thingArn</td>
<td>string</td>
<td>The ARN of the thing on which the job execution is running.</td>
</tr>
<tr>
<td>queuedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job execution was queued.</td>
</tr>
<tr>
<td>startedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job execution started.</td>
</tr>
<tr>
<td>lastUpdatedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job execution was last updated.</td>
</tr>
</tbody>
</table>
DescribeJobExecution

Gets details of a job execution.

https

Request syntax:

GET /things/thingName/jobs/jobId?
executionNumber=executionNumber&includeJobDocument=includeJobDocument

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>DescribeJobExecutionJobId</td>
<td>yes</td>
<td>The unique identifier assigned to this job when it was created.</td>
</tr>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The thing name associated with the device the job execution is running on.</td>
</tr>
</tbody>
</table>
AWS IoT Developer Guide
DescribeJobExecution

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>includeJobDocument</td>
<td>IncludeJobDocument</td>
<td>no</td>
<td>Optional. When set to true, the response contains the job document. The default is false.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>ExecutionNumber</td>
<td>no</td>
<td>Optional. A number that identifies a particular job execution on a particular device. If not specified, the latest job execution is returned.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```json
{
    "execution": {
        "jobId": "string",
        "thingName": "string",
        "status": "string",
        "statusDetails": {
            "string": "string"
        },
        "queuedAt": "long",
        "startedAt": "long",
        "lastUpdatedAt": "long",
        "versionNumber": "long",
        "executionNumber": "long",
        "jobDocument": "string"
    }
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>execution</td>
<td>JobExecution</td>
<td>no</td>
<td>Contains data about a job execution.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.
HTTP response code: 404
ThrottlingException
   The rate exceeds the limit.

HTTP response code: 429
ServiceUnavailableException
   The service is temporarily unavailable.

HTTP response code: 503
CertificateValidationException
   The certificate is invalid.

HTTP response code: 400
TerminalStateException
   The job is in a terminal state.

HTTP response code: 410

cli

Synopsis:

```
aws iot-jobs-data describe-job-execution \
 --job-id <value> \
 --thing-name <value> \
 [--include-job-document | --no-include-job-document] \
 [--execution-number <value>] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "jobId": "string",
   "thingName": "string",
   "includeJobDocument": "boolean",
   "executionNumber": "long"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td>^$next</td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The thing name associated with the device the job execution is running on.</td>
</tr>
<tr>
<td></td>
<td>length= max:128 min:1</td>
<td>pattern: [a-zA-Z0-9-_]+</td>
</tr>
</tbody>
</table>
### Name | Type | Description
---|---|---
includeJobDocument | boolean | Optional. When set to true, the response contains the job document. The default is false.
executionNumber | long | Optional. A number that identifies a particular job execution on a particular device. If not specified, the latest job execution is returned.

#### Output:

```
{  
  "execution": {  
    "jobId": "string",  
    "thingName": "string",  
    "status": "string",  
    "statusDetails": {  
      "string": "string"  
    },  
    "queuedAt": "long",  
    "startedAt": "long",  
    "lastUpdatedAt": "long",  
    "versionNumber": "long",  
    "executionNumber": "long",  
    "jobDocument": "string"  
  }  
}
```

#### cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>execution</td>
<td>JobExecution</td>
<td>Contains data about a job execution.</td>
</tr>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created. length- max:64 min:1 pattern: [a-zA-Z0-9-_.]+</td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing that is executing the job. length- max:128 min:1 pattern: [a-zA-Z0-9-_.]+</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the job execution. Can be one of: &quot;QUEUED&quot;, &quot;IN_PROGRESS&quot;, &quot;FAILED&quot;, &quot;SUCCESS&quot;, &quot;CANCELED&quot;, &quot;REJECTED&quot;, or &quot;REMOVED&quot;. enum: QUEUED</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>statusDetails</td>
<td>map</td>
<td>A collection of name/value pairs that describe the status of the job execution.</td>
</tr>
<tr>
<td>queuedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was enqueued.</td>
</tr>
<tr>
<td>startedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was started.</td>
</tr>
<tr>
<td>lastUpdatedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was last updated.</td>
</tr>
<tr>
<td>versionNumber</td>
<td>long</td>
<td>The version of the job execution. Job execution versions are incremented each time they are updated by a device.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>long</td>
<td>A number that identifies a particular job execution on a particular device. It can be used later in commands that return or update job execution information.</td>
</tr>
<tr>
<td>jobDocument</td>
<td>string</td>
<td>The content of the job document.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceNotFoundException

The specified resource does not exist.

ThrottlingException

The rate exceeds the limit.

ServiceUnavailableException

The service is temporarily unavailable.

CertificateValidationException

The certificate is invalid.

TerminalStateException

The job is in a terminal state.
DescribeRoleAlias

Describes a role alias.

https

Request syntax:

GET /role-aliases/roleAlias

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleAlias</td>
<td>RoleAlias</td>
<td>yes</td>
<td>The role alias to describe.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```
{
  "roleAliasDescription": {
    "roleAlias": "string",
    "roleAliasArn": "string",
    "roleArn": "string",
    "owner": "string",
    "credentialDurationSeconds": "integer",
    "creationDate": "timestamp",
    "lastModifiedDate": "timestamp"
  }
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleAliasDescription</td>
<td>RoleAliasDescription</td>
<td>no</td>
<td>The role alias description.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429
UnauthorizedException
You are not authorized to perform this operation.
HTTP response code: 401
ServiceUnavailableException
The service is temporarily unavailable.
HTTP response code: 503
InternalFailureException
An unexpected error has occurred.
HTTP response code: 500
ResourceNotFoundException
The specified resource does not exist.
HTTP response code: 404

cli

Synopsis:

```
aws iot describe-role-alias \
   --role-alias <value> \ 
   [--cli-input-json <value>] \ 
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "roleAlias": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleAlias</td>
<td>string</td>
<td>The role alias to describe.</td>
</tr>
</tbody>
</table>

length- max:128 min:1
pattern: [w=,@-]+

Output:

```
{
   "roleAliasDescription": {
      "roleAlias": "string",
      "roleAliasArn": "string",
      "roleArn": "string",
      "owner": "string",
      "credentialDurationSeconds": "integer",
      "creationDate": "timestamp",
      "lastModifiedDate": "timestamp"
   }
}
```
cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleAliasDescription</td>
<td>RoleAliasDescription</td>
<td>The role alias description.</td>
</tr>
<tr>
<td>roleAlias</td>
<td>string</td>
<td>The role alias.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w=,@-]+</td>
<td></td>
</tr>
<tr>
<td>roleAliasArn</td>
<td>string</td>
<td>The ARN of the role alias.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The role ARN.</td>
</tr>
<tr>
<td></td>
<td>length- max:2048 min:20</td>
<td></td>
</tr>
<tr>
<td>owner</td>
<td>string</td>
<td>The role alias owner.</td>
</tr>
<tr>
<td></td>
<td>length- max:12 min:12</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [0-9]+</td>
<td></td>
</tr>
<tr>
<td>credentialDurationSeconds</td>
<td>integer</td>
<td>The number of seconds for which the credential is valid.</td>
</tr>
<tr>
<td></td>
<td>range- max:3600 min:900</td>
<td></td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The UNIX timestamp of when the role alias was created.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>timestamp</td>
<td>The UNIX timestamp of when the role alias was last modified.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

ResourceNotFoundException

The specified resource does not exist.
DescribeScheduledAudit

Gets information about a scheduled audit.

https

Request syntax:

GET /audit/scheduledaudits/scheduledAuditName

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditName</td>
<td>ScheduledAuditName</td>
<td>yes</td>
<td>The name of the scheduled audit whose information you want to get.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{
  "frequency": "string",
  "dayOfMonth": "string",
  "dayOfWeek": "string",
  "targetCheckNames": [
    "string"
  ],
  "scheduledAuditName": "string",
  "scheduledAuditArn": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>AuditFrequency</td>
<td>no</td>
<td>How often the scheduled audit takes place. One of &quot;DAILY&quot;, &quot;WEEKLY&quot;, &quot;BIWEEKLY&quot; or &quot;MONTHLY&quot;. The actual start time of each audit is determined by the system.</td>
</tr>
<tr>
<td>dayOfMonth</td>
<td>DayOfMonth</td>
<td>no</td>
<td>The day of the month on which the scheduled audit takes place. Will be &quot;1&quot; through &quot;31&quot; or &quot;LAST&quot;. If days 29-31 are specified, and the</td>
</tr>
</tbody>
</table>
### Name

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditName</td>
<td>ScheduledAuditName</td>
<td>no</td>
<td>The name of the scheduled audit.</td>
</tr>
<tr>
<td>targetCheckNames</td>
<td>TargetAuditCheckNames</td>
<td>no</td>
<td>Which checks are performed during the scheduled audit. (Note that checks must be enabled for your account. (Use DescribeAccountAuditConfiguration to see the list of all checks including those that are enabled or UpdateAccountAuditConfiguration to select which checks are enabled.)</td>
</tr>
<tr>
<td>dayOfWeek</td>
<td>DayOfWeek</td>
<td>no</td>
<td>The day of the week on which the scheduled audit takes place. One of “SUN”, “MON”, “TUE”, “WED”, “THU”, “FRI” or “SAT”.</td>
</tr>
<tr>
<td>scheduledAuditArn</td>
<td>ScheduledAuditArn</td>
<td>no</td>
<td>The ARN of the scheduled audit.</td>
</tr>
</tbody>
</table>

### Errors:

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**InternalFailureException**

An unexpected error has occurred.
HTTP response code: 500

cli

Synopsis:

```
aws iot describe-scheduled-audit \
  --scheduled-audit-name <value>  \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "scheduledAuditName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditName</td>
<td>string</td>
<td>The name of the scheduled audit whose information you want to get.</td>
</tr>
</tbody>
</table>

Output:

```
{
  "frequency": "string",
  "dayOfMonth": "string",
  "dayOfWeek": "string",
  "targetCheckNames": [
    "string"
  ],
  "scheduledAuditName": "string",
  "scheduledAuditArn": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>string</td>
<td>How often the scheduled audit takes place. One of &quot;DAILY&quot;, &quot;WEEKLY&quot;, &quot;BIWEEKLY&quot; or &quot;MONTHLY&quot;. The actual start time of each audit is determined by the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: DAILY</td>
</tr>
<tr>
<td>dayOfMonth</td>
<td>string</td>
<td>The day of the month on which the scheduled audit takes</td>
</tr>
</tbody>
</table>
## DescribeSecurityProfile

### Name | Type | Description
---|---|---
| dayOfWeek | string | The day of the week on which the scheduled audit takes place. One of "SUN", "MON", "TUE", "WED", "THU", "FRI" or "SAT". enum: SUN | MON | TUE | WED | THU | FRI | SAT

targetCheckNames | list | Which checks are performed during the scheduled audit. (Note that checks must be enabled for your account. (Use DescribeAccountAuditConfiguration to see the list of all checks including those that are enabled or UpdateAccountAuditConfiguration to select which checks are enabled.)

erscheduledAuditName | string | The name of the scheduled audit.
length- max:128 min:1
pattern: [a-zA-Z0-9-_]+
scheduledAuditArn | string | The ARN of the scheduled audit.

### Errors:

- **InvalidRequestException**
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ResourceNotFoundException**
  The specified resource does not exist.

- **ThrottlingException**
  The rate exceeds the limit.

- **InternalFailureException**
  An unexpected error has occurred.

### DescribeSecurityProfile

Gets information about a Device Defender security profile.
https

Request syntax:

GET /security-profiles/{securityProfileName}

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>yes</td>
<td>The name of the security profile whose information you want to get.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```
{
  "securityProfileName": "string",
  "securityProfileArn": "string",
  "securityProfileDescription": "string",
  "behaviors": [
    {
      "name": "string",
      "metric": "string",
      "criteria": {
        "comparisonOperator": "string",
        "value": {
          "count": "long",
          "cidsrs": [
            "string"
          ],
          "ports": [
            "integer"
          ],
          "durationSeconds": "integer"
        }
      }
    },
    "alertTargets": {
      "String": {
        "alertTargetArn": "string",
        "roleArn": "string"
      }
    },
    "version": "long",
    "creationDate": "timestamp",
    "lastModifiedDate": "timestamp"
  }
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>no</td>
<td>The name of the security profile.</td>
</tr>
</tbody>
</table>
DescribeSecurityProfile

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileArn</td>
<td>SecurityProfileArn</td>
<td>no</td>
<td>The ARN of the security profile.</td>
</tr>
<tr>
<td>securityProfileDescription</td>
<td>SecurityProfileDescription</td>
<td>no</td>
<td>A description of the security profile (associated with the security profile when it was created or updated).</td>
</tr>
<tr>
<td>behaviors</td>
<td>Behaviors</td>
<td>no</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td>alertTargets</td>
<td>AlertTargets</td>
<td>no</td>
<td>Where the alerts are sent. (Alerts are always sent to the console.)</td>
</tr>
<tr>
<td>version</td>
<td>Version</td>
<td>no</td>
<td>The version of the security profile. A new version is generated whenever the security profile is updated.</td>
</tr>
<tr>
<td>creationDate</td>
<td>Timestamp</td>
<td>no</td>
<td>The time the security profile was created.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>Timestamp</td>
<td>no</td>
<td>The time the security profile was last modified.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500
cli

Synopsis:

```
aws iot describe-security-profile \
--security-profile-name <value> \ 
[--cli-input-json <value>] \ 
[--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "securityProfileName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name of the security profile whose information you want to get.</td>
</tr>
<tr>
<td>length-</td>
<td>max:128</td>
<td>min:1</td>
</tr>
<tr>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Output:

```
{
  "securityProfileName": "string",
  "securityProfileArn": "string",
  "securityProfileDescription": "string",
  "behaviors": [
    {
      "name": "string",
      "metric": "string",
      "criteria": {
        "comparisonOperator": "string",
        "value": {
          "count": "long",
          "cidrs": [ "string" ],
          "ports": [ "integer" ]
        },
        "durationSeconds": "integer"
      }
    },
    "alertTargets": {
      "string": {
        "alertTargetArn": "string",
        "roleArn": "string"
      }
    },
    "version": "long",
    "creationDate": "timestamp",
    "lastModifiedDate": "timestamp"
  }
}
```
## DescribeSecurityProfile

### cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name of the security profile.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>securityProfileArn</td>
<td>string</td>
<td>The ARN of the security profile.</td>
</tr>
<tr>
<td>securityProfileDescription</td>
<td>string</td>
<td>A description of the security profile (associated with the security profile when it was created or updated).</td>
</tr>
<tr>
<td></td>
<td>length- max:1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: \p{Graph} *</td>
<td></td>
</tr>
<tr>
<td>behaviors</td>
<td>list</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the behavior.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>metric</td>
<td>string</td>
<td>What is measured by the behavior.</td>
</tr>
<tr>
<td>criteria</td>
<td>BehaviorCriteria</td>
<td>The criteria that determine if a device is behaving normally in regard to the metric.</td>
</tr>
<tr>
<td>comparisonOperator</td>
<td>string</td>
<td>The operator that relates the thing measured (metric) to the criteria (value).</td>
</tr>
<tr>
<td></td>
<td>enum: less-than</td>
<td>less-than-equals</td>
</tr>
<tr>
<td>value</td>
<td>MetricValue</td>
<td>The value to be compared with the metric.</td>
</tr>
<tr>
<td>count</td>
<td>long</td>
<td>If the comparisonOperator calls for a numeric value, use this to specify that numeric value to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>range- min:0</td>
<td></td>
</tr>
<tr>
<td>cidrs</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of CIDRs, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>member: Cidr</td>
<td></td>
</tr>
</tbody>
</table>
## DescribeStream

**Name** | **Type** | **Description**
---|---|---
ports | list member: Port | If the `comparisonOperator` calls for a set of ports, use this to specify that set to be compared with the metric.
durationSeconds | integer | Use this to specify the period of time over which the behavior is evaluated, for those criteria which have a time dimension (for example, `NUM_MESSAGES_SENT`).
alertTargets | map | Where the alerts are sent. (Alerts are always sent to the console.)
alertTargetArn | string | The ARN of the notification target to which alerts are sent.
roleArn | string length- max:2048 min:20 | The ARN of the role that grants permission to send alerts to the notification target.
version | long | The version of the security profile. A new version is generated whenever the security profile is updated.
creationDate | timestamp | The time the security profile was created.
lastModifiedDate | timestamp | The time the security profile was last modified.

**Errors:**

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an `UpdateJobExecution` request contains invalid status details. The message contains details about the error.

- **ResourceNotFoundException**
  
  The specified resource does not exist.

- **ThrottlingException**
  
  The rate exceeds the limit.

- **InternalFailureException**
  
  An unexpected error has occurred.

### DescribeStream

Gets information about a stream.
https

Request syntax:

GET /streams/streamId

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streamId</td>
<td>StreamId</td>
<td>yes</td>
<td>The stream ID.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```
{
  "streamInfo": {
    "streamId": "string",
    "streamArn": "string",
    "streamVersion": "integer",
    "description": "string",
    "files": [
      {
        "fileId": "integer",
        "s3Location": {
          "bucket": "string",
          "key": "string",
          "version": "string"
        }
      }
    ],
    "createdAt": "timestamp",
    "lastUpdatedAt": "timestamp",
    "roleArn": "string"
  }
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streamInfo</td>
<td>StreamInfo</td>
<td>no</td>
<td>Information about the stream.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.
HTTP response code: 404
ThrottlingException
The rate exceeds the limit.

HTTP response code: 429
UnauthorizedException
You are not authorized to perform this operation.

HTTP response code: 401
ServiceUnavailableException
The service is temporarily unavailable.

HTTP response code: 503
InternalFailureException
An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```bash
cli

aws iot describe-stream
  --stream-id <value> 
  [--cli-input-json <value>] 
  [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "streamId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streamId</td>
<td>string</td>
<td>The stream ID.</td>
</tr>
</tbody>
</table>

length- max:128 min:1

pattern: [a-zA-Z0-9-_.]+

Output:

```json
{
  "StreamInfo": {
    "streamId": "string",
    "streamArn": "string",
    "streamVersion": "integer",
    "description": "string",
    "files": [
      {
      }
DescribeStream

```json
"fileId": "integer",
"s3Location": {
  "bucket": "string",
  "key": "string",
  "version": "string"
}
},
"createdAt": "timestamp",
"lastUpdatedAt": "timestamp",
"roleArn": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streamInfo</td>
<td>StreamInfo</td>
<td>Information about the stream.</td>
</tr>
<tr>
<td>streamId</td>
<td>string</td>
<td>The stream ID.</td>
</tr>
<tr>
<td>streamArn</td>
<td>string</td>
<td>The stream ARN.</td>
</tr>
<tr>
<td>streamVersion</td>
<td>integer</td>
<td>The stream version.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>The description of the stream.</td>
</tr>
<tr>
<td>files</td>
<td>list</td>
<td>The files to stream.</td>
</tr>
<tr>
<td>fileld</td>
<td>integer</td>
<td>The file ID.</td>
</tr>
<tr>
<td>s3Location</td>
<td>S3Location</td>
<td>The location of the file in S3.</td>
</tr>
<tr>
<td>bucket</td>
<td>string</td>
<td>The S3 bucket that contains the file to stream.</td>
</tr>
<tr>
<td>key</td>
<td>string</td>
<td>The name of the file within the S3 bucket to stream.</td>
</tr>
<tr>
<td>version</td>
<td>string</td>
<td>The file version.</td>
</tr>
<tr>
<td>createdAt</td>
<td>timestamp</td>
<td>The date when the stream was created.</td>
</tr>
<tr>
<td>lastUpdatedAt</td>
<td>timestamp</td>
<td>The date when the stream was last updated.</td>
</tr>
</tbody>
</table>
DescribeThing

Gets information about the specified thing.

Request syntax:

GET /things/thingName

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{
  "defaultClientId": "string",
  "thingName": "string",
  "thingId": "string",
  "thingArn": "string",
}
"thingTypeName": "string",
"attributes": {
   "string": "string"
},
"version": "long"

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>defaultClientId</td>
<td>ClientId</td>
<td>no</td>
<td>The default client ID.</td>
</tr>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>no</td>
<td>The name of the thing.</td>
</tr>
<tr>
<td>thingId</td>
<td>ThingId</td>
<td>no</td>
<td>The ID of the thing to describe.</td>
</tr>
<tr>
<td>thingArn</td>
<td>ThingArn</td>
<td>no</td>
<td>The ARN of the thing to describe.</td>
</tr>
<tr>
<td>thingTypeName</td>
<td>ThingTypeName</td>
<td>no</td>
<td>The thing type name.</td>
</tr>
<tr>
<td>attributes</td>
<td>Attributes</td>
<td>no</td>
<td>The thing attributes.</td>
</tr>
<tr>
<td>version</td>
<td>Version</td>
<td>no</td>
<td>The current version of the thing record in the registry.</td>
</tr>
</tbody>
</table>

**Note**
To avoid unintentional changes to the information in the registry, you can pass the version information in the `expectedVersion` parameter of the UpdateThing and DeleteThing calls.

Errors:

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
HTTP response code: 400
ThrottlingException
The rate exceeds the limit.

HTTP response code: 429
UnauthorizedException
You are not authorized to perform this operation.

HTTP response code: 401
ServiceUnavailableException
The service is temporarily unavailable.

HTTP response code: 503
InternalFailureException
An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

aws iot describe-thing \ 
   --thing-name <value> \ 
   [--cli-input-json <value>] \ 
   [--generate-cli-skeleton]

cli-input-json format:

{"thingName": "string"}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing.</td>
</tr>
</tbody>
</table>

Output:

{"defaultClientId": "string",
 "thingName": "string",
 "thingId": "string",
 "thingArn": "string",
 "thingTypeName": "string"}
"attributes": {  
  "string": "string"
},
  "version": "long"
}

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>defaultClientId</td>
<td>string</td>
<td>The default client ID.</td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing.</td>
</tr>
<tr>
<td>thingId</td>
<td>string</td>
<td>The ID of the thing to describe.</td>
</tr>
<tr>
<td>thingArn</td>
<td>string</td>
<td>The ARN of the thing to describe.</td>
</tr>
<tr>
<td>thingTypeName</td>
<td>string</td>
<td>The thing type name.</td>
</tr>
<tr>
<td>attributes</td>
<td>map</td>
<td>The thing attributes.</td>
</tr>
<tr>
<td>version</td>
<td>long</td>
<td>The current version of the thing record in the registry.</td>
</tr>
</tbody>
</table>

**Note**
To avoid unintentional changes to the information in the registry, you can pass the version information in the expectedVersion parameter of the UpdateThing and DeleteThing calls.

**Errors:**

- **ResourceNotFoundException**
  
  The specified resource does not exist.

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ThrottlingException**
  
  The rate exceeds the limit.
UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

DescribeThingGroup

Describe a thing group.

https

Request syntax:

GET /thing-groups/thingGroupName

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>ThingGroupName</td>
<td>yes</td>
<td>The name of the thing group.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```
{
  "thingGroupName": "string",
  "thingGroupId": "string",
  "thingGroupArn": "string",
  "version": "long",
  "thingGroupProperties": {
    "thingGroupDescription": "string",
    "attributePayload": {
      "attributes": {
        "string": "string"
      },
      "merge": "boolean"
    }
  },
  "thingGroupMetadata": {
    "parentGroupName": "string",
    "rootToParentThingGroups": [
      {
        "groupName": "string",
        "groupArn": "string"
      }
    ],
    "creationDate": "timestamp"
  }
}
```
Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>ThingGroupName</td>
<td>no</td>
<td>The name of the thing group.</td>
</tr>
<tr>
<td>thingGroupId</td>
<td>ThingGroupId</td>
<td>no</td>
<td>The thing group ID.</td>
</tr>
<tr>
<td>thingGroupArn</td>
<td>ThingGroupArn</td>
<td>no</td>
<td>The thing group ARN.</td>
</tr>
<tr>
<td>version</td>
<td>Version</td>
<td>no</td>
<td>The version of the thing group.</td>
</tr>
<tr>
<td>thingGroupProperties</td>
<td>ThingGroupProperties</td>
<td>no</td>
<td>The thing group properties.</td>
</tr>
<tr>
<td>thingGroupMetadata</td>
<td>ThingGroupMetadata</td>
<td>no</td>
<td>Thing group metadata.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException
The rate exceeds the limit.

HTTP response code: 429

InternalFailureException
An unexpected error has occurred.

HTTP response code: 500

ResourceNotFoundException
The specified resource does not exist.

HTTP response code: 404

cli

Synopsis:

```
aws iot describe-thing-group \
  --thing-group-name <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "thingGroupName": "string"
}
```
**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>string</td>
<td>The name of the thing group.</td>
</tr>
<tr>
<td></td>
<td>length: max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
</tbody>
</table>

**Output:**

```json
{
  "thingGroupName": "string",
  "thingGroupId": "string",
  "thingGroupArn": "string",
  "version": "long",
  "thingGroupProperties": {
    "thingGroupDescription": "string",
    "attributePayload": {
      "attributes": {
        "string": "string"
      },
      "merge": "boolean"
    },
    "thingGroupMetadata": {
      "parentGroupName": "string",
      "rootToParentThingGroups": [
        {
          "groupName": "string",
          "groupArn": "string"
        }
      ],
      "creationDate": "timestamp"
    }
  }
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>string</td>
<td>The name of the thing group.</td>
</tr>
<tr>
<td></td>
<td>length: max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>thingGroupId</td>
<td>string</td>
<td>The thing group ID.</td>
</tr>
<tr>
<td></td>
<td>length: max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>thingGroupArn</td>
<td>string</td>
<td>The thing group ARN.</td>
</tr>
<tr>
<td>thingGroupProperties</td>
<td>ThingGroupProperties</td>
<td>The thing group properties.</td>
</tr>
<tr>
<td>thingGroupDescription</td>
<td>string</td>
<td>The thing group description.</td>
</tr>
</tbody>
</table>
### DescribeThingGroup

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>length- max:2028 pattern: [\p{Graph}]*</td>
<td>The thing group attributes in JSON format.</td>
</tr>
<tr>
<td>attributePayload</td>
<td>AttributePayload</td>
<td>The thing group attributes in JSON format.</td>
</tr>
<tr>
<td>attributes</td>
<td>map</td>
<td>A JSON string containing up to three key-value pair in JSON format. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{&quot;attributes&quot;: {&quot;string1&quot;: &quot;string2&quot;}}</td>
</tr>
<tr>
<td>merge</td>
<td>boolean</td>
<td>Specifies whether the list of attributes provided in the AttributePayload is merged with the attributes stored in the registry, instead of overwriting them.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To remove an attribute, call UpdateThing with an empty attribute value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The merge attribute is only valid when calling UpdateThing.</td>
</tr>
<tr>
<td>thingGroupMetadata</td>
<td>ThingGroupMetadata</td>
<td>Thing group metadata.</td>
</tr>
<tr>
<td>parentGroupName</td>
<td>string</td>
<td>The parent thing group name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>rootToParentThingGroups</td>
<td>list</td>
<td>The root parent thing group.</td>
</tr>
<tr>
<td></td>
<td>member: GroupNameAndArn java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>groupName</td>
<td>string</td>
<td>The group name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>groupArn</td>
<td>string</td>
<td>The group ARN.</td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The UNIX timestamp of when the thing group was created.</td>
</tr>
</tbody>
</table>

**Errors:**
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

ResourceNotFoundException

The specified resource does not exist.

---

DescribeThingRegistrationTask

Describes a bulk thing provisioning task.

https

Request syntax:

GET /thing-registration-tasks/taskId

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>TaskId</td>
<td>yes</td>
<td>The task ID.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{
  "taskId": "string",
  "creationDate": "timestamp",
  "lastModifiedDate": "timestamp",
  "templateBody": "string",
  "inputFileBucket": "string",
  "inputFileKey": "string",
  "roleArn": "string",
  "status": "string",
  "message": "string",
  "successCount": "integer",
  "failureCount": "integer",
  "percentageProgress": "integer"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>TaskId</td>
<td>no</td>
<td>The task ID.</td>
</tr>
</tbody>
</table>
### DescribeThingRegistrationTask

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>creationDate</td>
<td>CreationDate</td>
<td>no</td>
<td>The task creation date.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>LastModifiedDate</td>
<td>no</td>
<td>The date when the task was last modified.</td>
</tr>
<tr>
<td>templateBody</td>
<td>TemplateBody</td>
<td>no</td>
<td>The task's template.</td>
</tr>
<tr>
<td>inputFileBucket</td>
<td>RegistryS3BucketName</td>
<td>no</td>
<td>The S3 bucket that contains the input file.</td>
</tr>
<tr>
<td>inputFileKey</td>
<td>RegistryS3KeyName</td>
<td>no</td>
<td>The input file key.</td>
</tr>
<tr>
<td>roleArn</td>
<td>RoleArn</td>
<td>no</td>
<td>The role ARN that grants access to the input file bucket.</td>
</tr>
<tr>
<td>status</td>
<td>Status</td>
<td>no</td>
<td>The status of the bulk thing provisioning task.</td>
</tr>
<tr>
<td>message</td>
<td>ErrorMessage</td>
<td>no</td>
<td>The message.</td>
</tr>
<tr>
<td>successCount</td>
<td>Count</td>
<td>no</td>
<td>The number of things successfully provisioned.</td>
</tr>
<tr>
<td>failureCount</td>
<td>Count</td>
<td>no</td>
<td>The number of things that failed to be provisioned.</td>
</tr>
<tr>
<td>percentageProgress</td>
<td>Percentage</td>
<td>no</td>
<td>The progress of the bulk provisioning task expressed as a percentage.</td>
</tr>
</tbody>
</table>

**Errors:**

- **InvalidRequestException**
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  
  HTTP response code: 400

- **ThrottlingException**
  - The rate exceeds the limit.

  HTTP response code: 429

- **UnauthorizedException**
  - You are not authorized to perform this operation.

  HTTP response code: 401

- **InternalFailureException**
  - An unexpected error has occurred.

  HTTP response code: 500
ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

cli

Synopsis:

```
aws iot describe-thing-registration-task \
  --task-id <value>  \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "taskId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>string</td>
<td>The task ID.</td>
</tr>
<tr>
<td></td>
<td>length- max:40</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```
{
  "taskId": "string",
  "creationDate": "timestamp",
  "lastModifiedDate": "timestamp",
  "templateBody": "string",
  "inputFileBucket": "string",
  "inputFileKey": "string",
  "roleArn": "string",
  "status": "string",
  "message": "string",
  "successCount": "integer",
  "failureCount": "integer",
  "percentageProgress": "integer"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>string</td>
<td>The task ID.</td>
</tr>
<tr>
<td></td>
<td>length- max:40</td>
<td></td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The task creation date.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>timestamp</td>
<td>The date when the task was last modified.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>templateBody</td>
<td>string</td>
<td>The task's template.</td>
</tr>
<tr>
<td>inputFileBucket</td>
<td>string</td>
<td>The S3 bucket that contains the input file.</td>
</tr>
<tr>
<td>inputFileKey</td>
<td>string</td>
<td>The input file key.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The role ARN that grants access to the input file bucket.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the bulk thing provisioning task.</td>
</tr>
<tr>
<td>message</td>
<td>string</td>
<td>The message.</td>
</tr>
<tr>
<td>successCount</td>
<td>integer</td>
<td>The number of things successfully provisioned.</td>
</tr>
<tr>
<td>failureCount</td>
<td>integer</td>
<td>The number of things that failed to be provisioned.</td>
</tr>
<tr>
<td>percentageProgress</td>
<td>integer</td>
<td>The progress of the bulk provisioning task expressed as a percentage.</td>
</tr>
</tbody>
</table>

**Errors:**

- **InvalidRequestException**
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
- **ThrottlingException**
  The rate exceeds the limit.
- **UnauthorizedException**
  You are not authorized to perform this operation.
- **InternalFailureException**
  An unexpected error has occurred.
- **ResourceNotFoundException**
  The specified resource does not exist.
DescribeThingType

Gets information about the specified thing type.

https

Request syntax:

GET /thing-types/thingTypeName

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>ThingTypeName</td>
<td>yes</td>
<td>The name of the thing type.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```
{
    "thingTypeName": "string",
    "thingTypeId": "string",
    "thingTypeArn": "string",
    "thingTypeProperties": {
        "thingTypeDescription": "string",
        "searchableAttributes": [
            "string"
        ]
    },
    "thingTypeMetadata": {
        "deprecated": "boolean",
        "deprecationDate": "timestamp",
        "creationDate": "timestamp"
    }
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>ThingTypeName</td>
<td>no</td>
<td>The name of the thing type.</td>
</tr>
<tr>
<td>thingTypeId</td>
<td>ThingTypeId</td>
<td>no</td>
<td>The thing type ID.</td>
</tr>
<tr>
<td>thingTypeArn</td>
<td>ThingTypeArn</td>
<td>no</td>
<td>The thing type ARN.</td>
</tr>
<tr>
<td>thingTypeProperties</td>
<td>ThingTypeProperties</td>
<td>no</td>
<td>The ThingTypeProperties contains information about the thing type including description, and a list of searchable thing attribute names.</td>
</tr>
</tbody>
</table>
The `thingTypeMetadata` contains additional information about the thing type including:
creation date and time, a value indicating whether the thing type is deprecated, and a
date and time when it was deprecated.

Errors:

- **ResourceNotFoundException**
  
The specified resource does not exist.
  
  HTTP response code: 404

- **InvalidRequestException**
  
The contents of the request were invalid. For example, this code is returned when an
  UpdateJobExecution request contains invalid status details. The message contains details about the
  error.
  
  HTTP response code: 400

- **ThrottlingException**
  
The rate exceeds the limit.
  
  HTTP response code: 429

- **UnauthorizedException**
  
  You are not authorized to perform this operation.
  
  HTTP response code: 401

- **ServiceUnavailableException**
  
The service is temporarily unavailable.
  
  HTTP response code: 503

- **InternalFailureException**
  
  An unexpected error has occurred.
  
  HTTP response code: 500

cli

Synopsis:

```
aws iot describe-thing-type
  --thing-type-name <value>
  [--cli-input-json <value>]
  [--generate-cli-skeleton]
```
cli-input-json format:

```json
{
  "thingTypeName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>string</td>
<td>The name of the thing type.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9;_:-]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
  "thingTypeName": "string",
  "thingTypeId": "string",
  "thingTypeArn": "string",
  "thingTypeProperties": {
    "thingTypeDescription": "string",
    "searchableAttributes": ["string"
  ],
  "thingTypeMetadata": {
    "deprecated": "boolean",
    "deprecationDate": "timestamp",
    "creationDate": "timestamp"
  }
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>string</td>
<td>The name of the thing type.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9;_:-]+</td>
<td></td>
</tr>
<tr>
<td>thingTypeId</td>
<td>string</td>
<td>The thing type ID.</td>
</tr>
<tr>
<td>thingTypeArn</td>
<td>string</td>
<td>The thing type ARN.</td>
</tr>
<tr>
<td>thingTypeProperties</td>
<td>ThingTypeProperties</td>
<td>The ThingTypeProperties contains information about the thing type including description, and a list of searchable thing attribute names.</td>
</tr>
<tr>
<td>thingTypeDescription</td>
<td>string length- max:2028 pattern: [\p{Graph}]*</td>
<td>The description of the thing type.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>searchableAttributes</td>
<td>list</td>
<td>A list of searchable thing attribute names.</td>
</tr>
<tr>
<td></td>
<td>member: AttributeName</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>thingTypeMetadata</td>
<td>ThingTypeMetadata</td>
<td>The ThingTypeMetadata contains additional information about the thing type including: creation date and time, a value indicating whether the thing type is deprecated, and a date and time when it was deprecated.</td>
</tr>
<tr>
<td>deprecated</td>
<td>boolean</td>
<td>Whether the thing type is deprecated. If true, no new things could be associated with this type.</td>
</tr>
<tr>
<td>deprecationDate</td>
<td>timestamp</td>
<td>The date and time when the thing type was deprecated.</td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The date and time when the thing type was created.</td>
</tr>
</tbody>
</table>

**Errors:**

- **ResourceNotFoundException**
  - The specified resource does not exist.
- **InvalidRequestException**
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
- **ThrottlingException**
  - The rate exceeds the limit.
- **UnauthorizedException**
  - You are not authorized to perform this operation.
- **ServiceUnavailableException**
  - The service is temporarily unavailable.
- **InternalFailureException**
  - An unexpected error has occurred.

**DetachPolicy**

Detaches a policy from the specified target.
### https

**Request syntax:**

```
POST /target-policies/policyName
Content-type: application/json

{
  "target": "string"
}
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>yes</td>
<td>The policy to detach.</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>PolicyTarget</td>
<td>yes</td>
<td>The target from which the policy will be detached.</td>
</tr>
</tbody>
</table>

**Errors:**

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  
  HTTP response code: 400

- **ThrottlingException**
  
  The rate exceeds the limit.
  
  HTTP response code: 429

- **UnauthorizedException**
  
  You are not authorized to perform this operation.
  
  HTTP response code: 401

- **ServiceUnavailableException**
  
  The service is temporarily unavailable.
  
  HTTP response code: 503

- **InternalFailureException**
  
  An unexpected error has occurred.
  
  HTTP response code: 500
LimitExceededException

A limit has been exceeded.

HTTP response code: 410

cli

Synopsis:

```
aws iot detach-policy \\
--policy-name <value> \\
--target <value> \\
[--cli-input-json <value>] \\
[--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "policyName": "string",
  "target": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy to detach.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>length- max:128 min:1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pattern: [w+,.@-]+</td>
</tr>
<tr>
<td>target</td>
<td>string</td>
<td>The target from which the policy will be detached.</td>
</tr>
</tbody>
</table>

Output:

None

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.
InternalFailureException

An unexpected error has occurred.

LimitExceededException

A limit has been exceeded.

# DetachPrincipalPolicy

Removes the specified policy from the specified certificate.

**Note:** This API is deprecated. Please use DetachPolicy instead.

https

**Request syntax:**

```
DELETE /principal-policies/policyName
x-amzn-iot-principal: principal
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>yes</td>
<td>The name of the policy to detach.</td>
</tr>
<tr>
<td>principal</td>
<td>Principal</td>
<td>yes</td>
<td>The principal. If the principal is a certificate, specify the certificate ARN. If the principal is an Amazon Cognito identity, specify the identity ID.</td>
</tr>
</tbody>
</table>

**Errors:**

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.
HTTP response code: 429
UnauthorizedException
You are not authorized to perform this operation.

HTTP response code: 401
ServiceUnavailableException
The service is temporarily unavailable.

HTTP response code: 503
InternalFailureException
An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot detach-principal-policy \
   --policy-name <value> \
   --principal <value> \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "policyName": "string",
   "principal": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>string</td>
<td>The name of the policy to detach.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [w+=,.@-]+</td>
<td></td>
</tr>
<tr>
<td>principal</td>
<td>string</td>
<td>The principal. If the principal is a certificate, specify the certificate ARN. If the principal is an Amazon Cognito identity, specify the identity ID.</td>
</tr>
</tbody>
</table>

Output:

None

Errors:
ResourceNotFoundException

The specified resource does not exist.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

**DetachSecurityProfile**

Disassociates a Device Defender security profile from a thing group or from this account.

**https**

**Request syntax:**

```
DELETE /security-profiles/securityProfileName/targets?
securityProfileTargetArn=securityProfileTargetArn
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>yes</td>
<td>The security profile that is detached.</td>
</tr>
<tr>
<td>securityProfileTargetArn</td>
<td>SecurityProfileTargetArn</td>
<td>yes</td>
<td>The ARN of the thing group from which the security profile is detached.</td>
</tr>
</tbody>
</table>

**Errors:**

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400
ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

aws iot detach-security-profile \
  --security-profile-name <value> \
  --security-profile-target-arn <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]

cli-input-json format:

{  
  "securityProfileName": "string",  
  "securityProfileTargetArn": "string"  
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The security profile that is detached.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9:-_]+</td>
<td></td>
</tr>
<tr>
<td>securityProfileTargetArn</td>
<td>string</td>
<td>The ARN of the thing group from which the security profile is detached.</td>
</tr>
</tbody>
</table>

Output:

None

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
ResourceNotFoundException

The specified resource does not exist.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

## DetachThingPrincipal

Detaches the specified principal from the specified thing.

### HTTPS

### Request syntax:

```
DELETE /things/thingName/principals
x-amzn-principal: principal
```

### URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing.</td>
</tr>
<tr>
<td>principal</td>
<td>Principal</td>
<td>yes</td>
<td>If the principal is a certificate, this value must be ARN of the certificate. If the principal is an Amazon Cognito identity, this value must be the ID of the Amazon Cognito identity.</td>
</tr>
</tbody>
</table>

### Errors:

- **ResourceNotFoundException**
  - The specified resource does not exist.
  - HTTP response code: 404

- **InvalidRequestException**
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  - HTTP response code: 400

- **ThrottlingException**
  - The rate exceeds the limit.
HTTP response code: 429
UnauthorizedException
You are not authorized to perform this operation.

HTTP response code: 401
ServiceUnavailableException
The service is temporarily unavailable.

HTTP response code: 503
InternalFailureException
An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot detach-thing-principal \
  --thing-name <value> \
  --principal <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "thingName": "string",
  "principal": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing.</td>
</tr>
<tr>
<td></td>
<td>length: max:128 min:1 pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>principal</td>
<td>string</td>
<td>If the principal is a certificate, this value must be ARN of the certificate. If the principal is an Amazon Cognito identity, this value must be the ID of the Amazon Cognito identity.</td>
</tr>
</tbody>
</table>

Output:

None

Errors:
ResourceNotFoundException

The specified resource does not exist.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

## DisableTopicRule

Disables the rule.

https

### Request syntax:

POST /rules/ruleName/disable

### URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleName</td>
<td>RuleName</td>
<td>yes</td>
<td>The name of the rule to disable.</td>
</tr>
</tbody>
</table>

### Errors:

InternalException

An unexpected error has occurred.

HTTP response code: 500

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400
ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

cli

Synopsis:

```
aws iot disable-topic-rule \
  --rule-name <value>  \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "ruleName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleName</td>
<td>string</td>
<td>The name of the rule to disable.</td>
</tr>
<tr>
<td></td>
<td>length max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: ^[a-zA-Z0-9-]+$</td>
<td></td>
</tr>
</tbody>
</table>

Output:

None

Errors:

InternalException

An unexpected error has occurred.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ServiceUnavailableException

The service is temporarily unavailable.

UnauthorizedException

You are not authorized to perform this operation.
EnableTopicRule

Enables the rule.

https

Request syntax:

POST /rules/ruleName/enable

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleName</td>
<td>RuleName</td>
<td>yes</td>
<td>The name of the topic rule to enable.</td>
</tr>
</tbody>
</table>

Errors:

InternalException

An unexpected error has occurred.

HTTP response code: 500

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

cli

Synopsis:

aws iot enable-topic-rule \
  --rule-name <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]

cli-input-json format:

```json
{
  "ruleName": "string"
}
GetEffectivePolicies

Gets a list of the policies that have an effect on the authorization behavior of the specified device when it connects to the AWS IoT device gateway.

https

Request syntax:

```
POST /effective-policies?thingName=thingName
Content-type: application/json

{
  "principal": "string",
  "cognitoIdentityPoolId": "string"
}
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>no</td>
<td>The thing name.</td>
</tr>
</tbody>
</table>
Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>principal</td>
<td>Principal</td>
<td>no</td>
<td>The principal.</td>
</tr>
<tr>
<td>cognitoIdentityPoolId</td>
<td>CognitoIdentityPoolId</td>
<td>no</td>
<td>The Cognito identity pool ID.</td>
</tr>
</tbody>
</table>

Response syntax:

```
Content-type: application/json

{  
  "effectivePolicies": [  
    {  
      "policyName": "string",  
      "policyArn": "string",  
      "policyDocument": "string"  
    }  
  ]
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>effectivePolicies</td>
<td>EffectivePolicies</td>
<td>no</td>
<td>The effective policies.</td>
</tr>
</tbody>
</table>

Errors:

- ResourceNotFoundException
  - The specified resource does not exist.
  - HTTP response code: 404

- InvalidRequestException
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  - HTTP response code: 400

- ThrottlingException
  - The rate exceeds the limit.
  - HTTP response code: 429

- UnauthorizedException
  - You are not authorized to perform this operation.
  - HTTP response code: 401

- ServiceUnavailableException
  - The service is temporarily unavailable.
HTTP response code: 503
InternalFailureException
An unexpected error has occurred.

HTTP response code: 500
LimitExceededException
A limit has been exceeded.

HTTP response code: 410

cli

Synopsis:

```
aws iot  get-effective-policies \
    [--principal <value>] \ 
    [--cognito-identity-pool-id <value>] \ 
    [--thing-name <value>] \ 
    [--cli-input-json <value>] \ 
    [--generate-cli-skeleton]
```

cli-input-json format:

```
{
    "principal": "string",
    "cognitoIdentityPoolId": "string",
    "thingName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>principal</td>
<td>string</td>
<td>The principal.</td>
</tr>
<tr>
<td>cognitoIdentityPoolId</td>
<td>string</td>
<td>The Cognito identity pool ID.</td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The thing name.</td>
</tr>
<tr>
<td>length- max:128</td>
<td></td>
<td>max:128 min:1</td>
</tr>
<tr>
<td>pattern: [a-zA-Z0-9:._-]+</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Output:

```
{
    "effectivePolicies": [
        {
            "policyName": "string",
            "policyArn": "string",
            "policyDocument": "string"
        }
    ]
}
```
cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>effectivePolicies</td>
<td>list</td>
<td>The effective policies.</td>
</tr>
<tr>
<td></td>
<td>member: EffectivePolicy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w+=,.@-]+</td>
<td></td>
</tr>
<tr>
<td>policyArn</td>
<td>string</td>
<td>The policy ARN.</td>
</tr>
<tr>
<td>policyDocument</td>
<td>string</td>
<td>The IAM policy document.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException
The specified resource does not exist.

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException
The rate exceeds the limit.

UnauthorizedException
You are not authorized to perform this operation.

ServiceUnavailableException
The service is temporarily unavailable.

InternalFailureException
An unexpected error has occurred.

LimitExceededError
A limit has been exceeded.

GetIndexingConfiguration

Gets the search configuration.

https

Request syntax:
GET /indexing/config

Response syntax:

Content-type: application/json

{
  "thingIndexingConfiguration": {
    "thingIndexingMode": "string"
  }
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingIndexingConfiguration</td>
<td>ThingIndexingConfiguration</td>
<td>no</td>
<td>Thing indexing configuration.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot get-indexing-configuration
```
[--cli-input-json <value>] \
[--generate-cli-skeleton]

cli-input-json format:

{
}

Output:

{
  "thingIndexingConfiguration": {
    "thingIndexingMode": "string"
  }
}

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingIndexingConfiguration</td>
<td>ThingIndexingConfiguration</td>
<td>Thing indexing configuration.</td>
</tr>
</tbody>
</table>
| thingIndexingMode           | string                | Thing indexing mode. Valid values are:
|                             |                       | • REGISTRY – Your thing index will contain only registry data.             |
|                             |                       | • REGISTRY_AND_SHADOW - Your thing index will contain registry and shadow data. |
|                             |                       | • OFF - Thing indexing is disabled.                                        |
|                             |                       | enum: OFF | REGISTRY | REGISTRY_AND_SHADOW |

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.
GetJobDocument

Gets a job document.

https

Request syntax:

GET /jobs/jobId/job-document

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>JobId</td>
<td>yes</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{
  "document": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>document</td>
<td>JobDocument</td>
<td>no</td>
<td>The job document content.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429
ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

cli

Synopsis:

```bash
aws iot get-job-document \
   --job-id <value> \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
   "jobId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
   "document": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>document</td>
<td>string</td>
<td>The job document content.</td>
</tr>
<tr>
<td></td>
<td>length- max:32768</td>
<td></td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceNotFoundException

The specified resource does not exist.
GetLoggingOptions

Gets the logging options.

NOTE: use of this command is not recommended. Use GetV2LoggingOptions instead.

https

Request syntax:

GET /loggingOptions

Response syntax:

Content-type: application/json

{
  "roleArn": "string",
  "logLevel": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>AwsArn</td>
<td>no</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>logLevel</td>
<td>LogLevel</td>
<td>no</td>
<td>The logging level.</td>
</tr>
</tbody>
</table>

Errors:

InternalException

An unexpected error has occurred.

HTTP response code: 500

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503
cli

Synopsis:

```bash
aws iot get-logging-options \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

cli-input-json format:

```json
{
}
```

Output:

```json
{
   "roleArn": "string",
   "logLevel": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>logLevel</td>
<td>string</td>
<td>The logging level. enum: DEBUG</td>
</tr>
</tbody>
</table>

Errors:

- **InternalException**
  
  An unexpected error has occurred.

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ServiceUnavailableException**
  
  The service is temporarily unavailable.

GetOTAUpdate

Gets an OTA update.

https

Request syntax:
GET /otaUpdates/otaUpdateId

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>otaUpdateId</td>
<td>OTAUpdateId</td>
<td>yes</td>
<td>The OTA update ID.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{  
    "otaUpdateInfo": {  
        "otaUpdateId": "string", 
        "otaUpdateArn": "string", 
        "creationDate": "timestamp", 
        "lastModifiedDate": "timestamp", 
        "description": "string", 
        "targets": [  
            "string"  
        ], 
        "targetSelection": "string", 
        "otaUpdateFiles": [  
            {  
                "fileName": "string", 
                "fileVersion": "string", 
                "fileSource": {  
                    "streamId": "string", 
                    "fileId": "integer"  
                }, 
                "codeSigning": {  
                    "awsSignerJobId": "string", 
                    "customCodeSigning": {  
                        "signature": {  
                            "stream": {  
                                "streamId": "string", 
                                "fileId": "integer"  
                            }, 
                            "inlineDocument": "blob"  
                        }, 
                        "certificateChain": {  
                            "stream": {  
                                "streamId": "string", 
                                "fileId": "integer"  
                            }, 
                            "certificateName": "string", 
                            "inlineDocument": "string"  
                        },  
                        "hashAlgorithm": "string", 
                        "signatureAlgorithm": "string"  
                    }  
                }, 
                "attributes": {  
                    "string": "string"  
                }  
            }  
        ], 
        "otaUpdateStatus": "string", 
        "awsIotJobId": "string", 
        "awsIotJobArn": "string"  
    },  
    "otaUpdateJobToken": "string", 
    "otaUpdateJobStatus": "string"  
}
Responses:  

"errorInfo": {
  "code": "string",
  "message": "string"
},
"additionalParameters": {
  "string": "string"
}
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>otaUpdateInfo</td>
<td>OTAUpdateInfo</td>
<td>no</td>
<td>The OTA update info.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

cli

Synopsis:

```
aws iot get-ota-update \
  --ota-update-id <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```
cli-input-json format:

```
{
   "otaUpdateId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>otaUpdateId</td>
<td>string</td>
<td>The OTA update ID.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```
{
   "otaUpdateInfo": {
      "otaUpdateId": "string",
      "otaUpdateArn": "string",
      "creationDate": "timestamp",
      "lastModifiedDate": "timestamp",
      "description": "string",
      "targets": ["string"],
      "targetSelection": "string",
      "otaUpdateFiles": [
         {
            "fileName": "string",
            "fileVersion": "string",
            "fileSource": {
               "streamId": "string",
               "fileId": "integer"
            },
            "codeSigning": {
               "awsSignerJobId": "string",
               "customCodeSigning": {
                  "signature": {
                     "stream": {
                        "streamId": "string",
                        "fileId": "integer"
                     },
                     "inlineDocument": "blob"
                  },
                  "certificateChain": {
                     "stream": {
                        "streamId": "string",
                        "fileId": "integer"
                     },
                     "certificateName": "string",
                     "inlineDocument": "string"
                  },
                  "hashAlgorithm": "string",
                  "signatureAlgorithm": "string"
               }
            },
            "attributes": {
               "string": "string"
            }
         }
      ]
   }
}
```
GetOTAUpdate

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>otaUpdateInfo</td>
<td>OTAUpdateInfo</td>
<td>The OTA update info.</td>
</tr>
<tr>
<td>otaUpdateId</td>
<td>string</td>
<td>The OTA update ID.</td>
</tr>
<tr>
<td>otaUpdateArn</td>
<td>string</td>
<td>The OTA update ARN.</td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The date when the OTA update was created.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>timestamp</td>
<td>The date when the OTA update was last updated.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>A description of the OTA update.</td>
</tr>
<tr>
<td>targets</td>
<td>list</td>
<td>The targets of the OTA update.</td>
</tr>
<tr>
<td>targetSelection</td>
<td>string</td>
<td>Specifies whether the OTA update will continue to run (CONTINUOUS), or will complete after all those things specified as targets have completed the OTA update (SNAPSHOT). If continuous, the OTA update may also be run on a thing when a change is detected in a target. For example, an OTA update will run on a thing when the thing is added to a target group, even after the OTA update was completed by all things originally in the group.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>otaUpdateFiles</td>
<td>list</td>
<td>A list of files associated with the OTA update.</td>
</tr>
<tr>
<td>fileName</td>
<td>string</td>
<td>The name of the file.</td>
</tr>
<tr>
<td>fileVersion</td>
<td>string</td>
<td>The file version.</td>
</tr>
<tr>
<td>fileSource</td>
<td>Stream</td>
<td>The source of the file.</td>
</tr>
<tr>
<td>streamId</td>
<td>string</td>
<td>The stream ID.</td>
</tr>
<tr>
<td>fileId</td>
<td>integer</td>
<td>The ID of a file associated with a stream.</td>
</tr>
<tr>
<td>awsSignerJobId</td>
<td>string</td>
<td>The ID of the AWSSignerJob which was created to sign the file.</td>
</tr>
<tr>
<td>signature</td>
<td>CodeSigningSignature</td>
<td>The signature for the file.</td>
</tr>
<tr>
<td>stream</td>
<td>Stream</td>
<td>A stream of the code signing signature.</td>
</tr>
<tr>
<td>streamId</td>
<td>string</td>
<td>The stream ID.</td>
</tr>
<tr>
<td>fileId</td>
<td>integer</td>
<td>The ID of a file associated with a stream.</td>
</tr>
<tr>
<td>inlineDocument</td>
<td>blob</td>
<td>A base64 encoded binary representation of the code signing signature.</td>
</tr>
<tr>
<td>certificateChain</td>
<td>CodeSigningCertificateChain</td>
<td>The certificate chain.</td>
</tr>
<tr>
<td>stream</td>
<td>Stream</td>
<td>A stream of the certificate chain files.</td>
</tr>
</tbody>
</table>
**AWS IoT Developer Guide**

**GetOTAUpdate**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streamId</td>
<td>string</td>
<td>The stream ID.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9_-]+</td>
<td></td>
</tr>
<tr>
<td>fileId</td>
<td>integer</td>
<td>The ID of a file associated with a stream.</td>
</tr>
<tr>
<td>certificateName</td>
<td>string</td>
<td>The name of the certificate.</td>
</tr>
<tr>
<td>inlineDocument</td>
<td>string</td>
<td>A base64 encoded binary representation of the code signing certificate chain.</td>
</tr>
<tr>
<td>hashAlgorithm</td>
<td>string</td>
<td>The hash algorithm used to code sign the file.</td>
</tr>
<tr>
<td>signatureAlgorithm</td>
<td>string</td>
<td>The signature algorithm used to code sign the file.</td>
</tr>
<tr>
<td>attributes</td>
<td>map</td>
<td>A list of name/attribute pairs.</td>
</tr>
<tr>
<td>otaUpdateStatus</td>
<td>string</td>
<td>The status of the OTA update.</td>
</tr>
<tr>
<td></td>
<td>enum: CREATE_PENDING</td>
<td>CREATE_IN_PROGRESS</td>
</tr>
<tr>
<td>awsIotJobId</td>
<td>string</td>
<td>The AWS IoT job ID associated with the OTA update.</td>
</tr>
<tr>
<td>awsIotJobArn</td>
<td>string</td>
<td>The AWS IoT job ARN associated with the OTA update.</td>
</tr>
<tr>
<td>errorInfo</td>
<td>ErrorInfo</td>
<td>Error information associated with the OTA update.</td>
</tr>
<tr>
<td>code</td>
<td>string</td>
<td>The error code.</td>
</tr>
<tr>
<td>message</td>
<td>string</td>
<td>The error message.</td>
</tr>
<tr>
<td>additionalParameters</td>
<td>map</td>
<td>A collection of name/value pairs</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

**ThrottlingException**

The rate exceeds the limit.
UnauthorizedException
You are not authorized to perform this operation.

InternalFailureException
An unexpected error has occurred.

ServiceUnavailableException
The service is temporarily unavailable.

ResourceNotFoundException
The specified resource does not exist.

GetPendingJobExecutions

Gets the list of all jobs for a thing that are not in a terminal status.

https

Request syntax:

GET /things/thingName/jobs

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing that is executing the job.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{  
  "inProgressJobs": [  
    {  
      "jobId": "string",  
      "queuedAt": "long",  
      "startedAt": "long",  
      "lastUpdatedAt": "long",  
      "versionNumber": "long",  
      "executionNumber": "long"  
    }  
  ],  
  "queuedJobs": [  
    {  
      "jobId": "string",  
      "queuedAt": "long",  
      "startedAt": "long",  
      "lastUpdatedAt": "long",  
      "versionNumber": "long",  
      "executionNumber": "long"  
    }  
  ]
}
Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inProgressJobs</td>
<td>JobExecutionSummaryList</td>
<td>no</td>
<td>A list of JobExecutionSummary objects with status IN_PROGRESS.</td>
</tr>
<tr>
<td>queuedJobs</td>
<td>JobExecutionSummaryList</td>
<td>no</td>
<td>A list of JobExecutionSummary objects with status QUEUED.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

CertificateValidationException

The certificate is invalid.

HTTP response code: 400

cli

Synopsis:

```
aws iot-jobs-data get-pending-job-executions \
  --thing-name <value> \ 
  [--cli-input-json <value>] \ 
  [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "thingName": "string"
}
```
cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing that is executing the job.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td>pattern: [a-zA-Z0-9-_]+</td>
</tr>
</tbody>
</table>

Output:

```json
{
  "inProgressJobs": [
    {
      "jobId": "string",
      "queuedAt": "long",
      "startedAt": "long",
      "lastUpdatedAt": "long",
      "versionNumber": "long",
      "executionNumber": "long"
    }
  ],
  "queuedJobs": [
    {
      "jobId": "string",
      "queuedAt": "long",
      "startedAt": "long",
      "lastUpdatedAt": "long",
      "versionNumber": "long",
      "executionNumber": "long"
    }
  ]
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inProgressJobs</td>
<td>list</td>
<td>A list of JobExecutionSummary objects with status IN_PROGRESS.</td>
</tr>
<tr>
<td></td>
<td>member: JobExecutionSummary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>jobld</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:1</td>
<td>pattern: [a-zA-Z0-9-_]+</td>
</tr>
<tr>
<td>queuedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was enqueued.</td>
</tr>
<tr>
<td>startedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution started.</td>
</tr>
</tbody>
</table>
### GetPendingJobExecutions

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lastUpdatedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was last updated.</td>
</tr>
<tr>
<td>versionNumber</td>
<td>long</td>
<td>The version of the job execution. Job execution versions are incremented each time AWS IoT Jobs receives an update from a device.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>long</td>
<td>A number that identifies a particular job execution on a particular device.</td>
</tr>
<tr>
<td>queuedJobs</td>
<td>list</td>
<td>A list of JobExecutionSummary objects with status QUEUED.</td>
</tr>
<tr>
<td>jobld</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td>length- max:64 min:1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pattern: [a-zA-Z0-9_-]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>queuedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was enqueued.</td>
</tr>
<tr>
<td>startedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution started.</td>
</tr>
<tr>
<td>lastUpdatedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was last updated.</td>
</tr>
<tr>
<td>versionNumber</td>
<td>long</td>
<td>The version of the job execution. Job execution versions are incremented each time AWS IoT Jobs receives an update from a device.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>long</td>
<td>A number that identifies a particular job execution on a particular device.</td>
</tr>
</tbody>
</table>

**Errors:**

```InvalidRequestException```

The contents of the request were invalid. For example, this code is returned when an `UpdateJobExecution` request contains invalid status details. The message contains details about the error.
ResourceNotFoundException
  The specified resource does not exist.
ThrottlingException
  The rate exceeds the limit.
ServiceUnavailableException
  The service is temporarily unavailable.
CertificateValidationException
  The certificate is invalid.

GetPolicy

Gets information about the specified policy with the policy document of the default version.

https

Request syntax:

GET /policies/{policyName}

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>yes</td>
<td>The name of the policy.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{
  "policyName": "string",
  "policyArn": "string",
  "policyDocument": "string",
  "defaultVersionId": "string",
  "creationDate": "timestamp",
  "lastModifiedDate": "timestamp",
  "generationId": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>no</td>
<td>The policy name.</td>
</tr>
<tr>
<td>policyArn</td>
<td>PolicyArn</td>
<td>no</td>
<td>The policy ARN.</td>
</tr>
<tr>
<td>policyDocument</td>
<td>PolicyDocument</td>
<td>no</td>
<td>The JSON document that describes the policy.</td>
</tr>
</tbody>
</table>

833
### Name

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>defaultVersionId</td>
<td>PolicyVersionId</td>
<td>no</td>
<td>The default policy version ID.</td>
</tr>
<tr>
<td>creationDate</td>
<td>DateType</td>
<td>no</td>
<td>The date the policy was created.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>DateType</td>
<td>no</td>
<td>The date the policy was last modified.</td>
</tr>
<tr>
<td>generationId</td>
<td>GenerationId</td>
<td>no</td>
<td>The generation ID of the policy.</td>
</tr>
</tbody>
</table>

### Errors:

- **ResourceNotFoundException**
  - The specified resource does not exist.
  - HTTP response code: 404

- **InvalidRequestException**
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  - HTTP response code: 400

- **ThrottlingException**
  - The rate exceeds the limit.
  - HTTP response code: 429

- **UnauthorizedException**
  - You are not authorized to perform this operation.
  - HTTP response code: 401

- **ServiceUnavailableException**
  - The service is temporarily unavailable.
  - HTTP response code: 503

- **InternalFailureException**
  - An unexpected error has occurred.
  - HTTP response code: 500

### Synopsis:

```bash
aws iot get-policy \
  [--policy-name <value> \
  [--cli-input-json <value>]
```
GetPolicy

[--generate-cli-skeleton]

cli-input-json format:

```json
{
  "policyName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>string</td>
<td>The name of the policy.</td>
</tr>
<tr>
<td>length- max:128 min:1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pattern: [w+=,.@-]+</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
  "policyName": "string",
  "policyArn": "string",
  "policyDocument": "string",
  "defaultVersionId": "string",
  "creationDate": "timestamp",
  "lastModifiedDate": "timestamp",
  "generationId": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
<tr>
<td>length- max:128 min:1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pattern: [w+=,.@-]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>policyArn</td>
<td>string</td>
<td>The policy ARN.</td>
</tr>
<tr>
<td>policyDocument</td>
<td>string</td>
<td>The JSON document that describes the policy.</td>
</tr>
<tr>
<td>defaultVersionId</td>
<td>string</td>
<td>The default policy version ID.</td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The date the policy was created.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>timestamp</td>
<td>The date the policy was last modified.</td>
</tr>
<tr>
<td>generationId</td>
<td>string</td>
<td>The generation ID of the policy.</td>
</tr>
</tbody>
</table>

Errors:
GetPolicyVersion

Gets information about the specified policy version.

Request syntax:

GET /policies/policyName/version/policyVersionId

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>yes</td>
<td>The name of the policy.</td>
</tr>
<tr>
<td>policyVersionId</td>
<td>PolicyVersionId</td>
<td>yes</td>
<td>The policy version ID.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```json
{
  "policyArn": "string",
  "policyName": "string",
  "policyDocument": "string",
  "policyVersionId": "string",
  "isDefaultVersion": "boolean",
  "creationDate": "timestamp",
  "lastModifiedDate": "timestamp",
  "generationId": "string"
}
```
Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyArn</td>
<td>PolicyArn</td>
<td>no</td>
<td>The policy ARN.</td>
</tr>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>no</td>
<td>The policy name.</td>
</tr>
<tr>
<td>policyDocument</td>
<td>PolicyDocument</td>
<td>no</td>
<td>The JSON document that describes the policy.</td>
</tr>
<tr>
<td>policyVersionId</td>
<td>PolicyVersionId</td>
<td>no</td>
<td>The policy version ID.</td>
</tr>
<tr>
<td>isDefaultVersion</td>
<td>IsDefaultVersion</td>
<td>no</td>
<td>Specifies whether the policy version is the default.</td>
</tr>
<tr>
<td>creationDate</td>
<td>DateType</td>
<td>no</td>
<td>The date the policy version was created.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>DateType</td>
<td>no</td>
<td>The date the policy version was last modified.</td>
</tr>
<tr>
<td>generationId</td>
<td>GenerationId</td>
<td>no</td>
<td>The generation ID of the policy version.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException

  The specified resource does not exist.

  HTTP response code: 404

InvalidRequestException

  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

  HTTP response code: 400

ThrottlingException

  The rate exceeds the limit.

  HTTP response code: 429

UnauthorizedException

  You are not authorized to perform this operation.

  HTTP response code: 401

ServiceUnavailableException

  The service is temporarily unavailable.

  HTTP response code: 503

InternalFailureException

  An unexpected error has occurred.
HTTP response code: 500

cli

Synopsis:

```
aws iot get-policy-version \
   --policy-name <value> \
   --policy-version-id <value> \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "policyName": "string",
   "policyVersionId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>string</td>
<td>The name of the policy.</td>
</tr>
<tr>
<td></td>
<td>length-</td>
<td>max:128 min:1</td>
</tr>
<tr>
<td></td>
<td>pattern: [w+=,.@-]+</td>
<td></td>
</tr>
<tr>
<td>policyVersionId</td>
<td>string</td>
<td>The policy version ID.</td>
</tr>
<tr>
<td></td>
<td>pattern: [0-9]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```
{
   "policyArn": "string",
   "policyName": "string",
   "policyDocument": "string",
   "policyVersionId": "string",
   "isDefaultVersion": "boolean",
   "creationDate": "timestamp",
   "lastModifiedDate": "timestamp",
   "generationId": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyArn</td>
<td>string</td>
<td>The policy ARN.</td>
</tr>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
<tr>
<td></td>
<td>length-</td>
<td>max:128 min:1</td>
</tr>
<tr>
<td></td>
<td>pattern: [w+=,.@-]+</td>
<td></td>
</tr>
</tbody>
</table>
### GetRegistrationCode

Gets a registration code used to register a CA certificate with AWS IoT.

**https**

**Request syntax:**

```
GET /registrationcode
```

**Response syntax:**
Content-type: application/json
{
  "registrationCode": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>registrationCode</td>
<td>RegistrationCode</td>
<td>no</td>
<td>The CA certificate registration code.</td>
</tr>
</tbody>
</table>

Errors:

ThrottlingException
The rate exceeds the limit.
HTTP response code: 429

UnauthorizedException
You are not authorized to perform this operation.
HTTP response code: 401

ServiceUnavailableException
The service is temporarily unavailable.
HTTP response code: 503

InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
HTTP response code: 400

cli

Synopsis:

```
aws iot get-registration-code  
  [--cli-input-json <value>] 
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
}
```
Output:

```json
{
    "registrationCode": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>registrationCode</td>
<td>string</td>
<td>The CA certificate registration code.</td>
</tr>
<tr>
<td></td>
<td>length: max:64 min:64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: (0x)?[a-fA-F0-9]+</td>
<td></td>
</tr>
</tbody>
</table>

Errors:

- ThrottlingException
  The rate exceeds the limit.
- UnauthorizedException
  You are not authorized to perform this operation.
- ServiceUnavailableException
  The service is temporarily unavailable.
- InternalFailureException
  An unexpected error has occurred.
- InvalidRequestException
  The contents of the request were invalid. For example, this code is returned when an
  UpdateJobExecution request contains invalid status details. The message contains details about the
  error.

GetThingShadow

Gets the shadow for the specified thing.

For more information, see GetThingShadow in the AWS IoT Developer Guide.

https

Request syntax:

```
GET /things/thingName/shadow
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing.</td>
</tr>
</tbody>
</table>
**Response syntax:**

Content-type: application/json

```json
{
  "payload": "blob"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>payload</td>
<td>JsonDocument</td>
<td>no</td>
<td>The state information, in JSON format.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**UnauthorizedException**

You are not authorized to perform this operation.

HTTP response code: 401

**ServiceUnavailableException**

The service is temporarily unavailable.

HTTP response code: 503

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

**MethodNotAllowedException**

The specified combination of HTTP verb and URI is not supported.

HTTP response code: 405

**UnsupportedDocumentEncodingException**

The encoding is not supported.

HTTP response code: 415
cli

Synopsis:

```
aws iot-data get-thing-shadow \
--thing-name <value> \ 
[--cli-input-json <value>] \ 
[--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "thingName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing.</td>
</tr>
<tr>
<td></td>
<td>length: max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
  "payload": "blob"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>payload</td>
<td>blob</td>
<td>The state information, in JSON format.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ResourceNotFoundException

The specified resource does not exist.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.
ServiceUnavailableException
The service is temporarily unavailable.

InternalFailureException
An unexpected error has occurred.

MethodNotAllowedException
The specified combination of HTTP verb and URI is not supported.

UnsupportedDocumentEncodingException
The encoding is not supported.

GetTopicRule

Gets information about the rule.

https

Request syntax:

GET /rules/ruleName

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleName</td>
<td>RuleName</td>
<td>yes</td>
<td>The name of the rule.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{
  "ruleArn": "string",
  "rule": {
    "ruleName": "string",
    "sql": "string",
    "description": "string",
    "createdAt": "timestamp",
    "actions": [
      {
        "dynamoDB": {
          "tableName": "string",
          "roleArn": "string",
          "operation": "string",
          "hashKeyField": "string",
          "hashKeyValue": "string",
          "hashKeyType": "string",
          "rangeKeyField": "string",
          "rangeKeyValue": "string",
          "rangeKeyType": "string",
          "payloadField": "string"
        },
        "dynamoDBv2": {
          "roleArn": "string",
          "payloadField": "string"
        }
      }
    ]
  }
}
"putItem": {
  "tableName": "string"
},
"lambda": {
  "functionArn": "string"
},
"sns": {
  "targetArn": "string",
  "roleArn": "string",
  "messageFormat": "string"
},
"sqs": {
  "roleArn": "string",
  "queueUrl": "string",
  "useBase64": "boolean"
},
"kinesis": {
  "roleArn": "string",
  "streamName": "string",
  "partitionKey": "string"
},
"republish": {
  "roleArn": "string",
  "topic": "string"
},
"s3": {
  "roleArn": "string",
  "bucketName": "string",
  "key": "string",
  "cannedAcl": "string"
},
"firehose": {
  "roleArn": "string",
  "deliveryStreamName": "string",
  "separator": "string"
},
"cloudwatchMetric": {
  "roleArn": "string",
  "metricNamespace": "string",
  " metricName": "string",
  "metricValue": "string",
  "metricUnit": "string",
  "metricTimestamp": "string"
},
"cloudwatchAlarm": {
  "roleArn": "string",
  "alarmName": "string",
  "stateReason": "string",
  "stateValue": "string"
},
"elasticsearch": {
  "roleArn": "string",
  "endpoint": "string",
  "index": "string",
  "type": "string",
  "id": "string"
},
"salesforce": {
  "token": "string",
  "url": "string"
},
"iotAnalytics": {
  "channelArn": "string",
  "channelName": "string",
  "roleArn": "string"
"stepFunctions": {
  "executionNamePrefix": "string",
  "stateMachineName": "string",
  "roleArn": "string"
}
},
"ruleDisabled": "boolean",
"awsIoTSqlVersion": "string",
"errorAction": {
  "dynamoDB": {
    "tableName": "string",
    "roleArn": "string",
    "operation": "string",
    "hashKeyField": "string",
    "hashKeyValue": "string",
    "hashKeyType": "string",
    "rangeKeyField": "string",
    "rangeKeyValue": "string",
    "rangeKeyType": "string",
    "payloadField": "string"
  },
  "dynamoDBv2": {
    "roleArn": "string",
    "putItem": {
      "tableName": "string"
    }
  },
  "lambda": {
    "functionArn": "string"
  },
  "sns": {
    "targetArn": "string",
    "roleArn": "string",
    "messageFormat": "string"
  },
  "sqs": {
    "roleArn": "string",
    "queueUrl": "string",
    "useBase64": "boolean"
  },
  "kinesis": {
    "roleArn": "string",
    "streamName": "string",
    "partitionKey": "string"
  },
  "republish": {
    "roleArn": "string",
    "topic": "string"
  },
  "s3": {
    "roleArn": "string",
    "bucketName": "string",
    "key": "string",
    "cannedAcl": "string"
  },
  "firehose": {
    "roleArn": "string",
    "deliveryStreamName": "string",
    "separator": "string"
  },
  "cloudwatchMetric": {
    "roleArn": "string",
    "metricNamespace": "string",
    "metricName": "string"
  }
}
"metricValue": "string",
"metricUnit": "string",
"metricTimestamp": "string"
},
"cloudwatchAlarm": {
"roleArn": "string",
"alarmName": "string",
"stateReason": "string",
"stateValue": "string"
},
"elasticsearch": {
"roleArn": "string",
"endpoint": "string",
"index": "string",
"type": "string",
"id": "string"
},
"salesforce": {
"token": "string",
"url": "string"
},
"iotAnalytics": {
"channelArn": "string",
"channelName": "string",
"roleArn": "string"
},
"stepFunctions": {
"executionNamePrefix": "string",
"stateMachineName": "string",
"roleArn": "string"
}
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleArn</td>
<td>RuleArn</td>
<td>no</td>
<td>The rule ARN.</td>
</tr>
<tr>
<td>rule</td>
<td>TopicRule</td>
<td>no</td>
<td>The rule.</td>
</tr>
</tbody>
</table>

Errors:

InternalException

An unexpected error has occurred.

HTTP response code: 500

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503
UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

cli

Synopsis:

```bash
aws iot get-topic-rule \
  --rule-name <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "ruleName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleName</td>
<td>string</td>
<td>The name of the rule.</td>
</tr>
</tbody>
</table>

length- max:128 min:1

pattern: ^[a-zA-Z0-9_]+$

Output:

```json
{
  "ruleArn": "string",
  "rule": {
    "ruleName": "string",
    "sql": "string",
    "description": "string",
    "createdAt": "timestamp",
    "actions": [
      {
        "dynamoDB": {
          "tableName": "string",
          "roleArn": "string",
          "operation": "string",
          "hashKeyField": "string",
          "hashKeyValue": "string",
          "hashKeyType": "string",
          "rangeKeyField": "string",
          "rangeKeyValue": "string",
          "rangeKeyType": "string",
          "payloadField": "string"
        },
        "dynamoDBv2": {
          "roleArn": "string",
          "putItem": {
            "tableName": "string"
          }
        }
      }
    ]
  }
}
```
"executionNamePrefix": "string",
"stateMachineName": "string",
"roleArn": "string"
}
]
"ruleDisabled": "boolean",
"awsIotSqlVersion": "string",
"errorAction": {
  "dynamoDB": {
    "tableName": "string",
    "roleArn": "string",
    "operation": "string",
    "hashKeyField": "string",
    "hashKeyValue": "string",
    "hashKeyType": "string",
    "rangeKeyField": "string",
    "rangeKeyValue": "string",
    "rangeKeyType": "string",
    "payloadField": "string"
  },
  "dynamoDBv2": {
    "roleArn": "string",
    "putItem": {
      "tableName": "string"
    },
  },
  "lambda": {
    "functionArn": "string"
  },
  "sns": {
    "targetArn": "string",
    "roleArn": "string",
    "messageFormat": "string"
  },
  "sqs": {
    "roleArn": "string",
    "queueUrl": "string",
    "useBase64": "boolean"
  },
  "kinesis": {
    "roleArn": "string",
    "streamName": "string",
    "partitionKey": "string"
  },
  "republish": {
    "roleArn": "string",
    "topic": "string"
  },
  "s3": {
    "roleArn": "string",
    "bucketName": "string",
    "key": "string",
    "cannedAcl": "string"
  },
  "firehose": {
    "roleArn": "string",
    "deliveryStreamName": "string",
    "separator": "string"
  },
  "cloudwatchMetric": {
    "roleArn": "string",
    "metricNamespace": "string",
    "metricName": "string",
    "metricValue": "string",
    "metricUnit": "string"
"metricTimestamp": "string"
},
"cloudWatchAlarm": {
  "roleArn": "string",
  "alarmName": "string",
  "stateReason": "string",
  "stateValue": "string"
},
"elasticsearch": {
  "roleArn": "string",
  "endpoint": "string",
  "index": "string",
  "type": "string",
  "id": "string"
},
"salesforce": {
  "token": "string",
  "url": "string"
},
"iotAnalytics": {
  "channelArn": "string",
  "channelName": "string",
  "roleArn": "string"
},
"stepFunctions": {
  "executionNamePrefix": "string",
  "stateMachineName": "string",
  "roleArn": "string"
}
}
}

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleArn</td>
<td>string</td>
<td>The rule ARN.</td>
</tr>
<tr>
<td>rule</td>
<td>TopicRule</td>
<td>The rule.</td>
</tr>
<tr>
<td>ruleName</td>
<td>string</td>
<td>The name of the rule.</td>
</tr>
<tr>
<td>length-</td>
<td>max:128 min:1</td>
<td>The SQL statement used to query the topic. When using a SQL query with</td>
</tr>
<tr>
<td>pattern:</td>
<td></td>
<td>multiple lines, be sure to escape the newline characters.</td>
</tr>
<tr>
<td>sql</td>
<td>string</td>
<td>The SQL statement used to query the topic. When using a SQL query with</td>
</tr>
<tr>
<td></td>
<td></td>
<td>multiple lines, be sure to escape the newline characters.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>The description of the rule.</td>
</tr>
<tr>
<td>createdAt</td>
<td>timestamp</td>
<td>The date and time the rule was created.</td>
</tr>
<tr>
<td>actions</td>
<td>list</td>
<td>The actions associated with the rule.</td>
</tr>
<tr>
<td></td>
<td>member:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td></td>
</tr>
<tr>
<td>dynamoDB</td>
<td>DynamoDBAction</td>
<td>Write to a DynamoDB table.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>tableName</td>
<td>string</td>
<td>The name of the DynamoDB table.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the DynamoDB table.</td>
</tr>
<tr>
<td>operation</td>
<td>string</td>
<td>The type of operation to be performed. This follows the substitution template, so it can be $ operation, but the substitution must result in one of the following: INSERT, UPDATE, or DELETE.</td>
</tr>
<tr>
<td>hashKeyField</td>
<td>string</td>
<td>The hash key name.</td>
</tr>
<tr>
<td>hashKeyValue</td>
<td>string</td>
<td>The hash key value.</td>
</tr>
<tr>
<td>hashKeyType</td>
<td>string</td>
<td>The hash key type. Valid values are &quot;STRING&quot; or &quot;NUMBER&quot;.</td>
</tr>
<tr>
<td>rangeKeyField</td>
<td>string</td>
<td>The range key name.</td>
</tr>
<tr>
<td>rangeKeyValue</td>
<td>string</td>
<td>The range key value.</td>
</tr>
<tr>
<td>rangeKeyType</td>
<td>string</td>
<td>The range key type. Valid values are &quot;STRING&quot; or &quot;NUMBER&quot;.</td>
</tr>
<tr>
<td>payloadField</td>
<td>string</td>
<td>The action payload. This name can be customized.</td>
</tr>
<tr>
<td>dynamoDBv2</td>
<td>DynamoDBv2Action</td>
<td>Write to a DynamoDB table. This is a new version of the DynamoDB action. It allows you to write each attribute in an MQTT message payload into a separate DynamoDB column.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the DynamoDB table.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>putItem</td>
<td>PutItemInput</td>
<td>Specifies the DynamoDB table to which the message data will be written. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{ &quot;dynamoDBv2&quot;:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{ &quot;roleArn&quot;: &quot;aws:iam:12341251:my-role&quot; &quot;putItem&quot;:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{ &quot;tableName&quot;: &quot;my-table&quot; } } } } }</td>
</tr>
<tr>
<td>tableName</td>
<td>string</td>
<td>The table where the message data will be written.</td>
</tr>
<tr>
<td>lambda</td>
<td>LambdaAction</td>
<td>Invoke a Lambda function.</td>
</tr>
<tr>
<td>functionArn</td>
<td>string</td>
<td>The ARN of the Lambda function.</td>
</tr>
<tr>
<td>sns</td>
<td>SnsAction</td>
<td>Publish to an Amazon SNS topic.</td>
</tr>
<tr>
<td>targetArn</td>
<td>string</td>
<td>The ARN of the SNS topic.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
</tbody>
</table>
| messageFormat | string          | (Optional) The message format of the message to publish. Accepted values are "JSON" and "RAW". The default value of the attribute is "RAW". SNS uses this setting to determine if the payload should be parsed and relevant platform-specific bits of the payload should be extracted. To read more about SNS message formats, see http://docs.aws.amazon.com/sns/latest/dg/json-formats.html
<p>|             |                     | refer to their official documentation. |
| sqs         | SqsAction           | Publish to an Amazon SQS queue. |
| roleArn     | string              | The ARN of the IAM role that grants access. |
| queueUrl    | string              | The URL of the Amazon SQS queue. |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>useBase64</td>
<td>boolean</td>
<td>Specifies whether to use Base64 encoding.</td>
</tr>
<tr>
<td>kinesis</td>
<td>KinesisAction</td>
<td>Write data to an Amazon Kinesis stream.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the Amazon Kinesis stream.</td>
</tr>
<tr>
<td>streamName</td>
<td>string</td>
<td>The name of the Amazon Kinesis stream.</td>
</tr>
<tr>
<td>partitionKey</td>
<td>string</td>
<td>The partition key.</td>
</tr>
<tr>
<td>republish</td>
<td>RepublishAction</td>
<td>Publish to another MQTT topic.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>topic</td>
<td>string</td>
<td>The name of the MQTT topic.</td>
</tr>
<tr>
<td>s3</td>
<td>S3Action</td>
<td>Write to an Amazon S3 bucket.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>bucketName</td>
<td>string</td>
<td>The Amazon S3 bucket.</td>
</tr>
<tr>
<td>key</td>
<td>string</td>
<td>The object key.</td>
</tr>
<tr>
<td>cannedAcl</td>
<td>string</td>
<td>The Amazon S3 canned ACL that controls access to the object identified by the object key. For more information, see S3 canned ACLs.</td>
</tr>
<tr>
<td>firehose</td>
<td>FirehoseAction</td>
<td>Write to an Amazon Kinesis Firehose stream.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role that grants access to the Amazon Kinesis Firehose stream.</td>
</tr>
<tr>
<td>deliveryStreamName</td>
<td>string</td>
<td>The delivery stream name.</td>
</tr>
</tbody>
</table>
### Name | Type | Description
--- | --- | ---
separator | string | A character separator that will be used to separate records written to the Firehose stream. Valid values are: \n (newline), \t (tab), \\n (Windows newline), , (comma).

cloudwatchMetric | CloudwatchMetricAction | Capture a CloudWatch metric.

roleArn | string | The IAM role that allows access to the CloudWatch metric.

metricNamespace | string | The CloudWatch metric namespace name.

metricName | string | The CloudWatch metric name.

metricValue | string | The CloudWatch metric value.

metricUnit | string | The metric unit supported by CloudWatch.

metricTimestamp | string | An optional Unix timestamp.

cloudwatchAlarm | CloudwatchAlarmAction | Change the state of a CloudWatch alarm.

roleArn | string | The IAM role that allows access to the CloudWatch alarm.

alarmName | string | The CloudWatch alarm name.

stateReason | string | The reason for the alarm change.

stateValue | string | The value of the alarm state. Acceptable values are: OK, ALARM, INSUFFICIENT_DATA.

elasticsearch | ElasticsearchAction | Write data to an Amazon Elasticsearch Service domain.

roleArn | string | The IAM role ARN that has access to Elasticsearch.

endpoint | string | The endpoint of your Elasticsearch domain.

index | string | The Elasticsearch index where you want to store your data.

type | string | The type of document you are storing.

id | string | The unique identifier for the document you are storing.
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>salesforce</td>
<td>SalesforceAction</td>
<td>Send a message to a Salesforce IoT Cloud Input Stream.</td>
</tr>
<tr>
<td>token</td>
<td>string</td>
<td>The token used to authenticate access to the Salesforce IoT Cloud Input Stream. The token is available from the Salesforce IoT Cloud platform after creation of the Input Stream.</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>The URL exposed by the Salesforce IoT Cloud Input Stream. The URL is available from the Salesforce IoT Cloud platform after creation of the Input Stream.</td>
</tr>
<tr>
<td>iotAnalytics</td>
<td>IotAnalyticsAction</td>
<td>Sends message data to an AWS IoT Analytics channel.</td>
</tr>
<tr>
<td>channelArn</td>
<td>string</td>
<td>(deprecated) The ARN of the IoT Analytics channel to which message data will be sent.</td>
</tr>
<tr>
<td>channelName</td>
<td>string</td>
<td>The name of the IoT Analytics channel to which message data will be sent.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role which has a policy that grants IoT Analytics permission to send message data via IoT Analytics (iotanalytics:BatchPutMessage).</td>
</tr>
<tr>
<td>stepFunctions</td>
<td>StepFunctionsAction</td>
<td>Starts execution of a Step Functions state machine.</td>
</tr>
<tr>
<td>executionNamePrefix</td>
<td>string</td>
<td>(Optional) A name will be given to the state machine execution consisting of this prefix followed by a UUID. Step Functions automatically creates a unique name for each state machine execution if one is not provided.</td>
</tr>
<tr>
<td>stateMachineName</td>
<td>string</td>
<td>The name of the Step Functions state machine whose execution will be started.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants IoT permission to start execution of a state machine (&quot;Action&quot;:&quot;states:StartExecution&quot;).</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ruleDisabled</td>
<td>boolean</td>
<td>Specifies whether the rule is disabled.</td>
</tr>
<tr>
<td>awsIotSqlVersion</td>
<td>string</td>
<td>The version of the SQL rules engine to use when evaluating the rule.</td>
</tr>
<tr>
<td>errorAction</td>
<td>Action</td>
<td>The action to perform when an error occurs.</td>
</tr>
<tr>
<td>dynamoDB</td>
<td>DynamoDBAction</td>
<td>Write to a DynamoDB table.</td>
</tr>
<tr>
<td>tableName</td>
<td>string</td>
<td>The name of the DynamoDB table.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the DynamoDB table.</td>
</tr>
<tr>
<td>operation</td>
<td>string</td>
<td>The type of operation to be performed. This follows the substitution template, so it can be $operation, but the substitution must result in one of the following: INSERT, UPDATE, or DELETE.</td>
</tr>
<tr>
<td>hashKeyField</td>
<td>string</td>
<td>The hash key name.</td>
</tr>
<tr>
<td>hashKeyValue</td>
<td>string</td>
<td>The hash key value.</td>
</tr>
<tr>
<td>hashKeyType</td>
<td>string</td>
<td>The hash key type. Valid values are &quot;STRING&quot; or &quot;NUMBER&quot;</td>
</tr>
<tr>
<td>rangeKeyField</td>
<td>string</td>
<td>The range key name.</td>
</tr>
<tr>
<td>rangeKeyValue</td>
<td>string</td>
<td>The range key value.</td>
</tr>
<tr>
<td>rangeKeyType</td>
<td>string</td>
<td>The range key type. Valid values are &quot;STRING&quot; or &quot;NUMBER&quot;</td>
</tr>
<tr>
<td>payloadField</td>
<td>string</td>
<td>The action payload. This name can be customized.</td>
</tr>
<tr>
<td>dynamoDBv2</td>
<td>DynamoDBv2Action</td>
<td>Write to a DynamoDB table. This is a new version of the DynamoDB action. It allows you to write each attribute in an MQTT message payload into a separate DynamoDB column.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the DynamoDB table.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>putItem</td>
<td>PutItemInput</td>
<td>Specifies the DynamoDB table to which the message data will be written. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{ &quot;dynamoDBv2&quot;: { &quot;roleArn&quot;: &quot;aws:iam:12341251:my-role&quot; &quot;putItem&quot;: { &quot;tableName&quot;: &quot;my-table&quot; } } }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Each attribute in the message payload will be written to a separate column in the DynamoDB database.</td>
</tr>
<tr>
<td>tableName</td>
<td>string</td>
<td>The table where the message data will be written.</td>
</tr>
<tr>
<td>lambda</td>
<td>LambdaAction</td>
<td>Invoke a Lambda function.</td>
</tr>
<tr>
<td>functionArn</td>
<td>string</td>
<td>The ARN of the Lambda function.</td>
</tr>
<tr>
<td>sns</td>
<td>SnsAction</td>
<td>Publish to an Amazon SNS topic.</td>
</tr>
<tr>
<td>targetArn</td>
<td>string</td>
<td>The ARN of the SNS topic.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>messageFormat</td>
<td>string</td>
<td>(Optional) The message format of the message to publish. Accepted values are &quot;JSON&quot; and &quot;RAW&quot;. The default value of the attribute is &quot;RAW&quot;. SNS uses this setting to determine if the payload should be parsed and relevant platform-specific bits of the payload should be extracted. To read more about SNS message formats, see <a href="http://docs.aws.amazon.com/sns/latest/dg/json-formats.html">http://docs.aws.amazon.com/sns/latest/dg/json-formats.html</a> refer to their official documentation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: RAW</td>
</tr>
<tr>
<td>sqs</td>
<td>SqsAction</td>
<td>Publish to an Amazon SQS queue.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>queueUrl</td>
<td>string</td>
<td>The URL of the Amazon SQS queue.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>useBase64</td>
<td>boolean</td>
<td>Specifies whether to use Base64 encoding.</td>
</tr>
<tr>
<td>kinesis</td>
<td>KinesisAction</td>
<td>Write data to an Amazon Kinesis stream.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the Amazon Kinesis stream.</td>
</tr>
<tr>
<td>streamName</td>
<td>string</td>
<td>The name of the Amazon Kinesis stream.</td>
</tr>
<tr>
<td>partitionKey</td>
<td>string</td>
<td>The partition key.</td>
</tr>
<tr>
<td>republish</td>
<td>RepublishAction</td>
<td>Publish to another MQTT topic.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>topic</td>
<td>string</td>
<td>The name of the MQTT topic.</td>
</tr>
<tr>
<td>s3</td>
<td>S3Action</td>
<td>Write to an Amazon S3 bucket.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>bucketName</td>
<td>string</td>
<td>The Amazon S3 bucket.</td>
</tr>
<tr>
<td>key</td>
<td>string</td>
<td>The object key.</td>
</tr>
<tr>
<td>cannedAcl</td>
<td>string</td>
<td>The Amazon S3 canned ACL that controls access to the object identified by the object key. For more information, see S3 canned ACLs. enum: private</td>
</tr>
<tr>
<td>firehose</td>
<td>FirehoseAction</td>
<td>Write to an Amazon Kinesis Firehose stream.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role that grants access to the Amazon Kinesis Firehose stream.</td>
</tr>
<tr>
<td>deliveryStreamName</td>
<td>string</td>
<td>The delivery stream name.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>separator</td>
<td>string, pattern: ( [ ] )</td>
<td>A character separator that will be used to separate records written to the Firehose stream. Valid values are: \n (newline), \t (tab), \n\n (Windows newline), , (comma).</td>
</tr>
<tr>
<td>cloudwatchMetric</td>
<td>CloudwatchMetricAction</td>
<td>Capture a CloudWatch metric.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role that allows access to the CloudWatch metric.</td>
</tr>
<tr>
<td>metricNamespace</td>
<td>string</td>
<td>The CloudWatch metric namespace name.</td>
</tr>
<tr>
<td>metricName</td>
<td>string</td>
<td>The CloudWatch metric name.</td>
</tr>
<tr>
<td>metricValue</td>
<td>string</td>
<td>The CloudWatch metric value.</td>
</tr>
<tr>
<td>metricUnit</td>
<td>string</td>
<td>The metric unit supported by CloudWatch.</td>
</tr>
<tr>
<td>metricTimestamp</td>
<td>string</td>
<td>An optional Unix timestamp.</td>
</tr>
<tr>
<td>cloudwatchAlarm</td>
<td>CloudwatchAlarmAction</td>
<td>Change the state of a CloudWatch alarm.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role that allows access to the CloudWatch alarm.</td>
</tr>
<tr>
<td>alarmName</td>
<td>string</td>
<td>The CloudWatch alarm name.</td>
</tr>
<tr>
<td>stateReason</td>
<td>string</td>
<td>The reason for the alarm change.</td>
</tr>
<tr>
<td>stateValue</td>
<td>string</td>
<td>The value of the alarm state. Acceptable values are: OK, ALARM, INSUFFICIENT_DATA.</td>
</tr>
<tr>
<td>elasticsearch</td>
<td>ElasticsearchAction</td>
<td>Write data to an Amazon Elasticsearch Service domain.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role ARN that has access to Elasticsearch.</td>
</tr>
<tr>
<td>endpoint</td>
<td>string, pattern: https?://.*</td>
<td>The endpoint of your Elasticsearch domain.</td>
</tr>
<tr>
<td>index</td>
<td>string</td>
<td>The Elasticsearch index where you want to store your data.</td>
</tr>
<tr>
<td>type</td>
<td>string</td>
<td>The type of document you are storing.</td>
</tr>
<tr>
<td>id</td>
<td>string</td>
<td>The unique identifier for the document you are storing.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>salesforce</td>
<td>SalesforceAction</td>
<td>Send a message to a Salesforce IoT Cloud Input Stream.</td>
</tr>
<tr>
<td>token</td>
<td>string</td>
<td>The token used to authenticate access to the Salesforce IoT Cloud Input Stream. The token is available from the Salesforce IoT Cloud platform after creation of the Input Stream.</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>The URL exposed by the Salesforce IoT Cloud Input Stream. The URL is available from the Salesforce IoT Cloud platform after creation of the Input Stream.</td>
</tr>
<tr>
<td>iotAnalytics</td>
<td>IotAnalyticsAction</td>
<td>Sends message data to an AWS IoT Analytics channel.</td>
</tr>
<tr>
<td>channelArn</td>
<td>string</td>
<td>(deprecated) The ARN of the IoT Analytics channel to which message data will be sent.</td>
</tr>
<tr>
<td>channelName</td>
<td>string</td>
<td>The name of the IoT Analytics channel to which message data will be sent.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role which has a policy that grants IoT Analytics permission to send message data via IoT Analytics (iotanalytics:BatchPutMessage).</td>
</tr>
<tr>
<td>stepFunctions</td>
<td>StepFunctionsAction</td>
<td>Starts execution of a Step Functions state machine.</td>
</tr>
<tr>
<td>executionNamePrefix</td>
<td>string</td>
<td>(Optional) A name will be given to the state machine execution consisting of this prefix followed by a UUID. Step Functions automatically creates a unique name for each state machine execution if one is not provided.</td>
</tr>
<tr>
<td>stateMachineName</td>
<td>string</td>
<td>The name of the Step Functions state machine whose execution will be started.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants IoT permission to start execution of a state machine (&quot;Action&quot;:'states:StartExecution&quot;).</td>
</tr>
</tbody>
</table>
Errors:

InternalException
   An unexpected error has occurred.
InvalidRequestException
   The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
ServiceUnavailableException
   The service is temporarily unavailable.
UnauthorizedException
   You are not authorized to perform this operation.

GetV2LoggingOptions

Gets the fine grained logging options.

https

Request syntax:

GET /v2LoggingOptions

Response syntax:

Content-type: application/json
{
   "roleArn": "string",
   "defaultLogLevel": "string",
   "disableAllLogs": "boolean"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>AwsArn</td>
<td>no</td>
<td>The IAM role ARN AWS IoT uses to write to your CloudWatch logs.</td>
</tr>
<tr>
<td>defaultLogLevel</td>
<td>LogLevel</td>
<td>no</td>
<td>The default log level.</td>
</tr>
<tr>
<td>disableAllLogs</td>
<td>DisableAllLogs</td>
<td>no</td>
<td>Disables all logs.</td>
</tr>
</tbody>
</table>

Errors:

InternalException
   An unexpected error has occurred.

HTTP response code: 500
NotConfiguredException

The resource is not configured.
HTTP response code: 404

ServiceUnavailableException

The service is temporarily unavailable.
HTTP response code: 503

cli

Synopsis:

`aws iot get-v2-logging-options  
[--cli-input-json <value>] 
[--generate-cli-skeleton]`

cli-input-json format:

```
{
}
```

Output:

```
{
  "roleArn": "string",
  "defaultLogLevel": "string",
  "disableAllLogs": "boolean"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role ARN AWS IoT uses to write to your CloudWatch logs.</td>
</tr>
<tr>
<td>defaultLogLevel</td>
<td>string</td>
<td>The default log level.</td>
</tr>
<tr>
<td>disableAllLogs</td>
<td>boolean</td>
<td>Disables all logs.</td>
</tr>
</tbody>
</table>

Errors:

InternalException

An unexpected error has occurred.

NotConfiguredException

The resource is not configured.

ServiceUnavailableException

The service is temporarily unavailable.
ListActiveViolations

Lists the active violations for a given Device Defender security profile.

https

Request syntax:

GET /active-violations?
maxResults=maxResults&nextToken=nextToken&thingName=thingName&securityProfileName=securityProfileName

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>no</td>
<td>The name of the thing whose active violations are listed.</td>
</tr>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>no</td>
<td>The name of the Device Defender security profile for which violations are listed.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{
  "activeViolations": [
    {
      "violationId": "string",
      "thingName": "string",
      "securityProfileName": "string",
      "behavior": {
        "name": "string",
        "metric": "string",
        "criteria": {
          "comparisonOperator": "string",
          "value": {
            "count": "long",
            "cidrs": ["string"],
            "ports": ["integer"
          },
          "durationSeconds": "integer"
        }
      }
    }
  }
}


>,
"lastViolationValue": {
  "count": "long",
  "cidrs": [
    "string"
  ],
  "ports": [
    "integer"
  ],
  "lastViolationTime": "timestamp",
  "violationStartTime": "timestamp"
}
},
"nextToken": "string"
}

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>activeViolations</td>
<td>ActiveViolations</td>
<td>no</td>
<td>The list of active violations.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

**Synopsis:**
aws iot list-active-violations \
[--thing-name <value>] \
[--security-profile-name <value>] \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]

cli-input-json format:

```
{
  "thingName": "string",
  "securityProfileName": "string",
  "nextToken": "string",
  "maxResults": "integer"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing whose active violations are listed.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_.-]+</td>
<td></td>
</tr>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name of the Device Defender security profile for which violations are listed.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_.-]+</td>
<td></td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td></td>
<td>range- max:250 min:1</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```
{
  "activeViolations": [
    {
      "violationId": "string",
      "thingName": "string",
      "securityProfileName": "string",
      "behavior": {
        "name": "string",
        "metric": "string",
        "criteria": {
          "comparisonOperator": "string",
          "value": {
            "count": "long",
            "cidrs": [
              "string"
            ],
            "ports": [
              "integer"
            ]
          }
        }
      }
    }
  ]
}
```
cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>activeViolations</td>
<td>list</td>
<td>The list of active violations.</td>
</tr>
<tr>
<td></td>
<td>member: ActiveViolation</td>
<td></td>
</tr>
<tr>
<td>violationId</td>
<td>string</td>
<td>The ID of the active violation.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-]+</td>
<td></td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing responsible for the active violation.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The security profile whose behavior is in violation.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>behavior</td>
<td>Behavior</td>
<td>The behavior which is being violated.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the behavior.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>metric</td>
<td>string</td>
<td>What is measured by the behavior.</td>
</tr>
<tr>
<td>criteria</td>
<td>BehaviorCriteria</td>
<td>The criteria that determine if a device is behaving normally in regard to the metric.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>comparisonOperator</td>
<td>string</td>
<td>The operator that relates the thing measured (metric) to the criteria (value).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: less-than</td>
</tr>
<tr>
<td>value</td>
<td>MetricValue</td>
<td>The value to be compared with the metric.</td>
</tr>
<tr>
<td>count</td>
<td>long</td>
<td>If the comparisonOperator calls for a numeric value, use this to specify that numeric value to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>range- min:0</td>
</tr>
<tr>
<td>cidrs</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of CIDRs, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>member: Cidr</td>
<td></td>
</tr>
<tr>
<td>ports</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of ports, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>member: Port</td>
<td></td>
</tr>
<tr>
<td>durationSeconds</td>
<td>integer</td>
<td>Use this to specify the period of time over which the behavior is evaluated, for those criteria which have a time dimension (for example, &quot;NUM_MESSAGES_SENT&quot;).</td>
</tr>
<tr>
<td>lastViolationValue</td>
<td>MetricValue</td>
<td>The value of the metric (the measurement) which caused the most recent violation.</td>
</tr>
<tr>
<td>count</td>
<td>long</td>
<td>If the comparisonOperator calls for a numeric value, use this to specify that numeric value to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>range- min:0</td>
</tr>
<tr>
<td>cidrs</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of CIDRs, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>member: Cidr</td>
<td></td>
</tr>
<tr>
<td>ports</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of ports, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>member: Port</td>
<td></td>
</tr>
</tbody>
</table>
### ListAttachedPolicies

Lists the policies attached to the specified thing group.

**https**

**Request syntax:**

```
POST /attached-policies/target?recursive=recursive&pageSize=pageSize&marker=marker
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>PolicyTarget</td>
<td>yes</td>
<td>The group for which the policies will be listed.</td>
</tr>
<tr>
<td>recursive</td>
<td>Recursive</td>
<td>no</td>
<td>When true, recursively list attached policies.</td>
</tr>
<tr>
<td>marker</td>
<td>Marker</td>
<td>no</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>pageSize</td>
<td>PageSize</td>
<td>no</td>
<td>The maximum number of results to be returned per request.</td>
</tr>
</tbody>
</table>

**Errors:**

- **InvalidRequestException**
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ResourceNotFoundException**
  The specified resource does not exist.

- **ThrottlingException**
  The rate exceeds the limit.

- **InternalFailureException**
  An unexpected error has occurred.
Response syntax:

```
Content-type: application/json

{
  "policies": [
    {
      "policyName": "string",
      "policyArn": "string"
    }
  ],
  "nextMarker": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policies</td>
<td>Policies</td>
<td>no</td>
<td>The policies.</td>
</tr>
<tr>
<td>nextMarker</td>
<td>Marker</td>
<td>no</td>
<td>The token to retrieve the next set of results, or null if there are no more results.</td>
</tr>
</tbody>
</table>

Errors:

- ResourceNotFoundException
  - The specified resource does not exist.
  - HTTP response code: 404

- InvalidRequestException
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  - HTTP response code: 400

- ThrottlingException
  - The rate exceeds the limit.
  - HTTP response code: 429

- UnauthorizedException
  - You are not authorized to perform this operation.
  - HTTP response code: 401

- ServiceUnavailableException
  - The service is temporarily unavailable.
  - HTTP response code: 503

- InternalFailureException
  - An unexpected error has occurred.
HTTP response code: 500
LimitExceededException
A limit has been exceeded.
HTTP response code: 410

cli

Synopsis:

```
aws iot list-attached-policies \
   --target <value> \
   [--recursive | --no-recursive] \
   [--marker <value>] \
   [--page-size <value>] \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "target": "string",
  "recursive": "boolean",
  "marker": "string",
  "pageSize": "integer"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>string</td>
<td>The group for which the policies will be listed.</td>
</tr>
<tr>
<td>recursive</td>
<td>boolean</td>
<td>When true, recursively list attached policies.</td>
</tr>
<tr>
<td>marker</td>
<td>string</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>pageSize</td>
<td>integer</td>
<td>The maximum number of results to be returned per request.</td>
</tr>
</tbody>
</table>

Output:

```
{
  "policies": [
    {
      "policyName": "string",
      "policyArn": "string"
    }
  ],
  "nextMarker": "string"
}
```
cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policies</td>
<td>list</td>
<td>The policies.</td>
</tr>
<tr>
<td>member: Policy</td>
<td>java.util.List</td>
<td></td>
</tr>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w+,.@-]+</td>
<td></td>
</tr>
<tr>
<td>policyArn</td>
<td>string</td>
<td>The policy ARN.</td>
</tr>
<tr>
<td>nextMarker</td>
<td>string</td>
<td>The token to retrieve the next set of results, or null if there are no more results.</td>
</tr>
<tr>
<td></td>
<td>pattern: [A-Za-z0-9+/]{0,2}</td>
<td></td>
</tr>
</tbody>
</table>

Errors:

- ResourceNotFoundException
  The specified resource does not exist.
- InvalidRequestException
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
- ThrottlingException
  The rate exceeds the limit.
- UnauthorizedException
  You are not authorized to perform this operation.
- ServiceUnavailableException
  The service is temporarily unavailable.
- InternalFailureException
  An unexpected error has occurred.
- LimitExceeded
  A limit has been exceeded.

**ListAuditFindings**

Lists the findings (results) of a Device Defender audit or of the audits performed during a specified time period. (Findings are retained for 180 days.)

**https**

**Request syntax:**
POST /audit/findings
Content-type: application/json

{
    "taskId": "string",
    "checkName": "string",
    "resourceIdentifier": {
        "deviceCertificateId": "string",
        "caCertificateId": "string",
        "cognitoIdentityPoolId": "string",
        "clientId": "string",
        "policyVersionIdentifier": {
            "policyName": "string",
            "policyVersionId": "string"
        },
        "account": "string"
    },
    "maxResults": "integer",
    "nextToken": "string",
    "startTime": "timestamp",
    "endTime": "timestamp"
}

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>AuditTaskId</td>
<td>no</td>
<td>A filter to limit results to the audit with the specified ID. You must specify either the taskId or the startTime and endTime, but not both.</td>
</tr>
<tr>
<td>checkName</td>
<td>AuditCheckName</td>
<td>no</td>
<td>A filter to limit results to the findings for the specified audit check.</td>
</tr>
<tr>
<td>resourceIdentifier</td>
<td>ResourceIdentifier</td>
<td>no</td>
<td>Information identifying the non-compliant resource.</td>
</tr>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time. The default is 25.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>startTime</td>
<td>Timestamp</td>
<td>no</td>
<td>A filter to limit results to those found after the specified time. You must specify either the startTime and endTime or the taskId, but not both.</td>
</tr>
<tr>
<td>endTime</td>
<td>Timestamp</td>
<td>no</td>
<td>A filter to limit results to those found before the specified time. You must specify either the startTime and endTime or the taskId, but not both.</td>
</tr>
</tbody>
</table>
ListAuditFindings

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>must specify either the startTime and endTime or the taskId, but not both.</td>
</tr>
</tbody>
</table>

Response syntax:

```json
Content-type: application/json

{  "findings": [    {      "taskId": "string",      "checkName": "string",      "taskStartTime": "timestamp",      "findingTime": "timestamp",      "severity": "string",      "nonCompliantResource": {        "resourceType": "string",        "resourceIdentifier": {          "deviceCertificateId": "string",          "caCertificateId": "string",          "cognitoIdentityPoolId": "string",          "clientId": "string",          "policyVersionIdentifier": {            "policyName": "string",            "policyVersionId": "string"          },          "account": "string"        },        "additionalInfo": {          "string": "string"        }      },      "relatedResources": [        {          "resourceType": "string",          "resourceIdentifier": {            "deviceCertificateId": "string",            "caCertificateId": "string",            "cognitoIdentityPoolId": "string",            "clientId": "string",            "policyVersionIdentifier": {              "policyName": "string",              "policyVersionId": "string"            },            "account": "string"          },          "additionalInfo": {            "string": "string"          }        }      ],      "reasonForNonCompliance": "string",      "reasonForNonComplianceCode": "string"    },  "nextToken": "string" }
```
### Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>findings</td>
<td>AuditFindings</td>
<td>no</td>
<td>The findings (results) of the audit.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

### Errors:

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

### cli

#### Synopsis:

```bash
aws iot list-audit-findings
    [--task-id <value>]
    [--check-name <value>]
    [--resource-identifier <value>]
    [--max-results <value>]
    [--next-token <value>]
    [--start-time <value>]
    [--end-time <value>]
    [--cli-input-json <value>]
    [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
    "taskId": "string",
    "checkName": "string",
    "resourceIdentifier": {
        "deviceCertificateId": "string",
        "caCertificateId": "string",
        "cognitoIdentityPoolId": "string",
        "clientId": "string",
```

875
"policyVersionIdentifier": {
  "policyName": "string",
  "policyVersionId": "string"
},
"account": "string"
},
"maxResults": "integer",
"nextToken": "string",
"startTime": "timestamp",
"endTime": "timestamp"}

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>string</td>
<td>A filter to limit results to the audit with the specified ID. You must specify either the taskId or the startTime and endTime, but not both.</td>
</tr>
<tr>
<td>checkName</td>
<td>string</td>
<td>A filter to limit results to the findings for the specified audit check.</td>
</tr>
<tr>
<td>resourceIdentifier</td>
<td>ResourceIdentifier</td>
<td>Information identifying the non-compliant resource.</td>
</tr>
<tr>
<td>deviceCertificateId</td>
<td>string</td>
<td>The ID of the certificate attached to the resource.</td>
</tr>
<tr>
<td>caCertificateId</td>
<td>string</td>
<td>The ID of the CA certificate used to authorize the certificate.</td>
</tr>
<tr>
<td>cognitoIdentityPoolId</td>
<td>string</td>
<td>The ID of the Cognito Identity Pool.</td>
</tr>
<tr>
<td>clientId</td>
<td>string</td>
<td>The client ID.</td>
</tr>
<tr>
<td>policyVersionIdentifier</td>
<td>PolicyVersionIdentifier</td>
<td>The version of the policy associated with the resource.</td>
</tr>
<tr>
<td>policyName</td>
<td>string</td>
<td>The name of the policy.</td>
</tr>
<tr>
<td>policyVersionId</td>
<td>string</td>
<td>The ID of the version of the policy associated with the resource.</td>
</tr>
<tr>
<td>account</td>
<td>string</td>
<td>The account with which the resource is associated.</td>
</tr>
</tbody>
</table>
ListAuditFindings

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time. The default is 25.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>startTime</td>
<td>timestamp</td>
<td>A filter to limit results to those found after the specified time. You must specify either the startTime and endTime or the taskId, but not both.</td>
</tr>
<tr>
<td>endTime</td>
<td>timestamp</td>
<td>A filter to limit results to those found before the specified time. You must specify either the startTime and endTime or the taskId, but not both.</td>
</tr>
</tbody>
</table>

Output:

```json
{
    "findings": [ 
        {
            "taskId": "string",
            "checkName": "string",
            "taskStartTime": "timestamp",
            "findingTime": "timestamp",
            "severity": "string",
            "nonCompliantResource": {
                "resourceType": "string",
                "resourceIdentifier": {
                    "deviceCertificateId": "string",
                    "caCertificateId": "string",
                    "cognitoIdentityPoolId": "string",
                    "clientId": "string",
                    "policyVersionIdentifier": {
                        "policyName": "string",
                        "policyVersionId": "string"
                    },
                    "account": "string"
                },
                "additionalInfo": {
                    "string": "string"
                }
            },
            "relatedResources": [ 
                {
                    "resourceType": "string",
                    "resourceIdentifier": {
                        "deviceCertificateId": "string",
                        "caCertificateId": "string",
                        "cognitoIdentityPoolId": "string",
                        "clientId": "string",
                        "policyVersionIdentifier": {
                            "policyName": "string",
                            "policyVersionId": "string"
                        }
                    }
                }
            ]
        }
    ]
}
```
"account": "string",
"additionalInfo": {
  "string": "string"
}
},
"reasonForNonCompliance": "string",
"reasonForNonComplianceCode": "string"
},
"nextToken": "string"}

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>findings</td>
<td>list member: AuditFinding</td>
<td>The findings (results) of the audit.</td>
</tr>
<tr>
<td>taskId</td>
<td>string</td>
<td>The ID of the audit that generated this result (finding)</td>
</tr>
<tr>
<td></td>
<td>length- max:40 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-]+</td>
<td></td>
</tr>
<tr>
<td>checkName</td>
<td>string</td>
<td>The audit check that generated this result.</td>
</tr>
<tr>
<td>taskStartTime</td>
<td>timestamp</td>
<td>The time the audit started.</td>
</tr>
<tr>
<td>findingTime</td>
<td>timestamp</td>
<td>The time the result (finding) was discovered.</td>
</tr>
<tr>
<td>severity</td>
<td>string</td>
<td>The severity of the result (finding).</td>
</tr>
<tr>
<td></td>
<td>enum: CRITICAL</td>
<td>HIGH</td>
</tr>
<tr>
<td>nonCompliantResource</td>
<td>NonCompliantResource</td>
<td>The resource that was found to be non-compliant with the audit check.</td>
</tr>
<tr>
<td>resourceType</td>
<td>string</td>
<td>The type of the non-compliant resource.</td>
</tr>
<tr>
<td></td>
<td>enum: DEVICE_CERTIFICATE</td>
<td>CA_CERTIFICATE</td>
</tr>
<tr>
<td>resourceIdentifier</td>
<td>Resourceldentifier</td>
<td>Information identifying the non-compliant resource.</td>
</tr>
<tr>
<td>deviceCertificateId</td>
<td>string</td>
<td>The ID of the certificate attached to the resource.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:64</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>caCertificateId</td>
<td>string</td>
<td>The ID of the CA certificate used to authorize the certificate.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: (0x)?[a-fA-F0-9]+</td>
<td></td>
</tr>
<tr>
<td>cognitoIdentityPoolId</td>
<td>string</td>
<td>The ID of the Cognito Identity Pool.</td>
</tr>
<tr>
<td>clientId</td>
<td>string</td>
<td>The client ID.</td>
</tr>
<tr>
<td>policyVersionIdentifier</td>
<td>PolicyVersionIdentifier</td>
<td>The version of the policy associated with the resource.</td>
</tr>
<tr>
<td>policyName</td>
<td>string</td>
<td>The name of the policy.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w+=,.@-]+</td>
<td></td>
</tr>
<tr>
<td>policyVersionId</td>
<td>string</td>
<td>The ID of the version of the policy associated with the resource.</td>
</tr>
<tr>
<td></td>
<td>pattern: [0-9]+</td>
<td></td>
</tr>
<tr>
<td>account</td>
<td>string</td>
<td>The account with which the resource is associated.</td>
</tr>
<tr>
<td></td>
<td>length- max:12 min:12</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [0-9]+</td>
<td></td>
</tr>
<tr>
<td>additionalInfo</td>
<td>map</td>
<td>Additional information about the non-compliant resource.</td>
</tr>
<tr>
<td>relatedResources</td>
<td>list</td>
<td>The list of related resources.</td>
</tr>
<tr>
<td>resourceType</td>
<td>string</td>
<td>The type of resource.</td>
</tr>
<tr>
<td></td>
<td>enum: DEVICE_CERTIFICATE</td>
<td>CA_CERTIFICATE</td>
</tr>
<tr>
<td>resourceIdentifier</td>
<td>ResourceIdentifier</td>
<td>Information identifying the resource.</td>
</tr>
<tr>
<td>deviceCertificateId</td>
<td>string</td>
<td>The ID of the certificate attached to the resource.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: (0x)?[a-fA-F0-9]+</td>
<td></td>
</tr>
</tbody>
</table>
## ListAuditFindings

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>caCertificateId</td>
<td>string</td>
<td>The ID of the CA certificate used to authorize the certificate.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: (0x)?[a-fA-F0-9]+</td>
<td></td>
</tr>
<tr>
<td>cognitoIdentityPoolId</td>
<td>string</td>
<td>The ID of the Cognito Identity Pool.</td>
</tr>
<tr>
<td>clientId</td>
<td>string</td>
<td>The client ID.</td>
</tr>
<tr>
<td></td>
<td>string</td>
<td>The ID of the version of the policy associated with the resource.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w+=,.@-]+</td>
<td></td>
</tr>
<tr>
<td>policyVersionId</td>
<td>PolicyVersionIdentifier</td>
<td>The name of the policy.</td>
</tr>
<tr>
<td></td>
<td>string</td>
<td>The ID of the version of the policy associated with the resource.</td>
</tr>
<tr>
<td></td>
<td>pattern: [0-9]+</td>
<td></td>
</tr>
<tr>
<td>account</td>
<td>string</td>
<td>The account with which the resource is associated.</td>
</tr>
<tr>
<td></td>
<td>length- max:12 min:12</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [0-9]+</td>
<td></td>
</tr>
<tr>
<td>additionalInfo</td>
<td>map</td>
<td>Additional information about the resource.</td>
</tr>
<tr>
<td>reasonForNonCompliance</td>
<td>string</td>
<td>The reason the resource was non-compliant.</td>
</tr>
<tr>
<td>reasonForNonComplianceCode</td>
<td>string</td>
<td>A code which indicates the reason that the resource was non-compliant.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

### Errors:

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

**ThrottlingException**

The rate exceeds the limit.

**InternalFailureException**

An unexpected error has occurred.
ListAuditTasks

Lists the Device Defender audits that have been performed during a given time period.

Request syntax:

```
GET /audit/tasks?
maxResults=maxResults&nextToken=nextToken&taskStatus=taskStatus&taskType=taskType&startTime=startTime&endTime=endTime
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startTime</td>
<td>Timestamp</td>
<td>yes</td>
<td>The beginning of the time period. Note that audit information is retained for a limited time (180 days). Requesting a start time prior to what is retained results in an &quot;InvalidRequestException&quot;.</td>
</tr>
<tr>
<td>endTime</td>
<td>Timestamp</td>
<td>yes</td>
<td>The end of the time period.</td>
</tr>
<tr>
<td>taskType</td>
<td>AuditTaskType</td>
<td>no</td>
<td>A filter to limit the output to the specified type of audit: can be one of &quot;ON_DEMAND_AUDIT_TASK&quot; or &quot;SCHEDULED_AUDIT_TASK&quot;.</td>
</tr>
<tr>
<td>taskStatus</td>
<td>AuditTaskStatus</td>
<td>no</td>
<td>A filter to limit the output to audits with the specified completion status: can be one of &quot;IN_PROGRESS&quot;, &quot;COMPLETED&quot;, &quot;FAILED&quot; or &quot;CANCELED&quot;.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time. The default is 25.</td>
</tr>
</tbody>
</table>

Response syntax:
AWS IoT Developer Guide
ListAuditTasks

**Content-type:** application/json

```json
{
  "tasks": [
  {
    "taskId": "string",
    "taskStatus": "string",
    "taskType": "string"
  },
  ],
  "nextToken": "string"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tasks</td>
<td>AuditTaskMetadataList</td>
<td>no</td>
<td>The audits that were performed during the specified time period.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

**cli**

**Synopsis:**

```
aws iot list-audit-tasks \
  --start-time <value> \
  --end-time <value> \
  [--task-type <value>] \
  [--task-status <value>] \
  [--next-token <value>] \
  [--max-results <value>] \
  [--cli-input-json <value>] \
```
cli-input-json format:

```json
{
    "startTime": "timestamp",
    "endTime": "timestamp",
    "taskType": "string",
    "taskStatus": "string",
    "nextToken": "string",
    "maxResults": "integer"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startTime</td>
<td>timestamp</td>
<td>The beginning of the time period. Note that audit information is retained for a limited time (180 days). Requesting a start time prior to what is retained results in an &quot;InvalidRequestException&quot;.</td>
</tr>
<tr>
<td>endTime</td>
<td>timestamp</td>
<td>The end of the time period.</td>
</tr>
<tr>
<td>taskType</td>
<td>string</td>
<td>A filter to limit the output to the specified type of audit: can be one of &quot;ON_DEMAND_AUDIT_TASK&quot; or &quot;SCHEDULED_AUDIT_TASK&quot;. enum: ON_DEMAND_AUDIT_TASK</td>
</tr>
<tr>
<td>taskStatus</td>
<td>string</td>
<td>A filter to limit the output to audits with the specified completion status: can be one of &quot;IN_PROGRESS&quot;, &quot;COMPLETED&quot;, &quot;FAILED&quot; or &quot;CANCELED&quot;. enum: IN_PROGRESS</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time. The default is 25.</td>
</tr>
</tbody>
</table>

Output:

```json
{
    "tasks": [
```
```json
{
  "taskId": "string",
  "taskStatus": "string",
  "taskType": "string"
},
"nextToken": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tasks</td>
<td>list</td>
<td>The audits that were performed during the specified time period.</td>
</tr>
<tr>
<td></td>
<td>member: AuditTaskMetadata</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>taskId</td>
<td>string</td>
<td>The ID of this audit.</td>
</tr>
<tr>
<td></td>
<td>length: max:40 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-]+</td>
<td></td>
</tr>
<tr>
<td>taskStatus</td>
<td>string</td>
<td>The status of this audit: one of &quot;IN_PROGRESS&quot;, &quot;COMPLETED&quot;, &quot;FAILED&quot; or &quot;CANCELED&quot;.</td>
</tr>
<tr>
<td></td>
<td>enum: IN_PROGRESS</td>
<td>COMPLETED</td>
</tr>
<tr>
<td>taskType</td>
<td>string</td>
<td>The type of this audit: one of &quot;ON_DEMAND_AUDIT_TASK&quot; or &quot;SCHEDULED_AUDIT_TASK&quot;.</td>
</tr>
<tr>
<td></td>
<td>enum: ON_DEMAND_AUDIT_TASK</td>
<td>SCHEDULED_AUDIT_TASK</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.
ListAuthorizers

Lists the authorizers registered in your account.

https

Request syntax:

```
GET /authorizers/?
pageSize=pageSize&marker=marker&isAscendingOrder=ascendingOrder&status=status
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pageSize</td>
<td>PageSize</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td>marker</td>
<td>Marker</td>
<td>no</td>
<td>A marker used to get the next set of results.</td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>AscendingOrder</td>
<td>no</td>
<td>Return the list of authorizers in ascending alphabetical order.</td>
</tr>
<tr>
<td>status</td>
<td>AuthorizerStatus</td>
<td>no</td>
<td>The status of the list authorizers request.</td>
</tr>
</tbody>
</table>

Response syntax:

```
Content-type: application/json
{
    "authorizers": [
        {
            "authorizerName": "string",
            "authorizerArn": "string"
        }
    ],
    "nextMarker": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizers</td>
<td>Authorizers</td>
<td>no</td>
<td>The authorizers.</td>
</tr>
<tr>
<td>nextMarker</td>
<td>Marker</td>
<td>no</td>
<td>A marker used to get the next set of results.</td>
</tr>
</tbody>
</table>

Errors:
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

aws iot list-authorizers

[--page-size <value>] 
[--marker <value>] 
[--ascending-order | --no-ascending-order] 
[--status <value>] 
[--cli-input-json <value>] 
[--generate-cli-skeleton]

cli-input-json format:

{
  "pageSize": "integer",
  "marker": "string",
  "ascendingOrder": "boolean",
  "status": "string"
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pageSize</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td></td>
<td>range- max:250 min:1</td>
<td></td>
</tr>
<tr>
<td>marker</td>
<td>string</td>
<td>A marker used to get the next set of results.</td>
</tr>
<tr>
<td></td>
<td>pattern: [A-Za-z0-9+/]{0,2}</td>
<td></td>
</tr>
</tbody>
</table>
ListAuthorizers

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ascendingOrder</td>
<td>boolean</td>
<td>Return the list of authorizers in ascending alphabetical order.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the list authorizers request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: ACTIVE</td>
</tr>
</tbody>
</table>

Output:

```json
{
  "authorizers": [
    {
      "authorizerName": "string",
      "authorizerArn": "string"
    }
  ],
  "nextMarker": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizers</td>
<td>list</td>
<td>The authorizers.</td>
</tr>
<tr>
<td></td>
<td>member: AuthorizerSummary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>authorizerName</td>
<td>string</td>
<td>The authorizer name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w=,@-]+</td>
<td></td>
</tr>
<tr>
<td>authorizerArn</td>
<td>string</td>
<td>The authorizer ARN.</td>
</tr>
<tr>
<td>nextMarker</td>
<td>string</td>
<td>A marker used to get the next set of results.</td>
</tr>
<tr>
<td></td>
<td>pattern: [A-Za-z0-9+/]{0,2}</td>
<td></td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.
ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

ListCAcertificates

Lists the CA certificates registered for your AWS account.

The results are paginated with a default page size of 25. You can use the returned marker to retrieve additional results.

Request syntax:

```
GET /cacertificates?pageSize=pageSize&marker=marker&isAscendingOrder=ascendingOrder
```

URL Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pageSize</td>
<td>PageSize</td>
<td>no</td>
<td>The result page size.</td>
</tr>
<tr>
<td>marker</td>
<td>Marker</td>
<td>no</td>
<td>The marker for the next set of results.</td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>AscendingOrder</td>
<td>no</td>
<td>Determines the order of the results.</td>
</tr>
</tbody>
</table>

Response syntax:

```
Content-type: application/json

{
    "certificates": [
        {
            "certificateArn": "string",
            "certificateId": "string",
            "status": "string",
            "creationDate": "timestamp"
        }
    ],
    "nextMarker": "String"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificates</td>
<td>CACertificates</td>
<td>no</td>
<td>The CA certificates registered in your AWS account.</td>
</tr>
</tbody>
</table>
### ListCACertificates

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextMarker</td>
<td>Marker</td>
<td>no</td>
<td>The current position within the list of CA certificates.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**UnauthorizedException**

You are not authorized to perform this operation.

HTTP response code: 401

**ServiceUnavailableException**

The service is temporarily unavailable.

HTTP response code: 503

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

**cli**

**Synopsis:**

```
aws iot list-ca-certificates \  
    [--page-size <value>] \  
    [--marker <value>] \  
    [--ascending-order | --no-ascending-order] \  
    [--cli-input-json <value>] \  
    [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
    "pageSize": "integer",
    "marker": "string",
    "ascendingOrder": "boolean"
}
```

889
cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pageSize</td>
<td>integer</td>
<td>The result page size.</td>
</tr>
<tr>
<td></td>
<td>range- max:250 min:1</td>
<td></td>
</tr>
<tr>
<td>marker</td>
<td>string</td>
<td>The marker for the next set of results.</td>
</tr>
<tr>
<td></td>
<td>pattern: [A-Za-z0-9+/]+={0,2}</td>
<td></td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>boolean</td>
<td>Determines the order of the results.</td>
</tr>
</tbody>
</table>

Output:

```json
{
  "certificates": [
    {
      "certificateArn": "string",
      "certificateId": "string",
      "status": "string",
      "creationDate": "timestamp"
    }
  ],
  "nextMarker": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificates</td>
<td>list</td>
<td>The CA certificates registered in your AWS account.</td>
</tr>
<tr>
<td></td>
<td>member: CACertificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>certificateArn</td>
<td>string</td>
<td>The ARN of the CA certificate.</td>
</tr>
<tr>
<td>certificateId</td>
<td>string</td>
<td>The ID of the CA certificate.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: (0x)?[a-fA-F0-9]+</td>
<td></td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the CA certificate.</td>
</tr>
<tr>
<td></td>
<td>enum: ACTIVE</td>
<td>The status value REGISTER_INACTIVE is deprecated and should not be used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INACTIVE</td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The date the CA certificate was created.</td>
</tr>
<tr>
<td>nextMarker</td>
<td>string</td>
<td>The current position within the list of CA certificates.</td>
</tr>
</tbody>
</table>
**ListCertificates**

Lists the certificates registered in your AWS account.

The results are paginated with a default page size of 25. You can use the returned marker to retrieve additional results.

**https**

**Request syntax:**

```
GET /certificates?pageSize=pageSize&marker=marker&isAscendingOrder=ascendingOrder
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pageSize</td>
<td>PageSize</td>
<td>no</td>
<td>The result page size.</td>
</tr>
<tr>
<td>marker</td>
<td>Marker</td>
<td>no</td>
<td>The marker for the next set of results.</td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>AscendingOrder</td>
<td>no</td>
<td>Specifies the order for results. If True, the results are returned in ascending order, based on the creation date.</td>
</tr>
</tbody>
</table>

**Response syntax:**
Content-type: application/json

{
   "certificates": [
      {
         "certificateArn": "string",
         "certificateId": "string",
         "status": "string",
         "creationDate": "timestamp"
      }
   ],
   "nextMarker": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificates</td>
<td>Certificates</td>
<td>no</td>
<td>The descriptions of the certificates.</td>
</tr>
<tr>
<td>nextMarker</td>
<td>Marker</td>
<td>no</td>
<td>The marker for the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalServerError

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:
aws iot list-certificates \
    [--page-size <value>] \
    [--marker <value>] \
    [--ascending-order | --no-ascending-order] \n    [--cli-input-json <value>] \n    [--generate-cli-skeleton]

cli-input-json format:

{  
    "pageSize": "integer",
    "marker": "string",
    "ascendingOrder": "boolean"
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pageSize</td>
<td>integer</td>
<td>The result page size.</td>
</tr>
<tr>
<td></td>
<td>range- max:250 min:1</td>
<td></td>
</tr>
<tr>
<td>marker</td>
<td>string</td>
<td>The marker for the next set of results.</td>
</tr>
<tr>
<td></td>
<td>pattern: [A-Za-z0-9+/]+{0,2}</td>
<td></td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>boolean</td>
<td>Specifies the order for results. If True, the results are returned in ascending order, based on the creation date.</td>
</tr>
</tbody>
</table>

Output:

{  
    "certificates": [  
        {  
            "certificateArn": "string",
            "certificateId": "string",
            "status": "string",
            "creationDate": "timestamp"
        },
        {  
            "nextMarker": "string"
        }
    ]
}

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificates</td>
<td>list</td>
<td>The descriptions of the certificates.</td>
</tr>
<tr>
<td></td>
<td>member: Certificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>certificateArn</td>
<td>string</td>
<td>The ARN of the certificate.</td>
</tr>
</tbody>
</table>
List the device certificates signed by the specified CA certificate.

https

Request syntax:
GET /certificates-by-ca/caCertificateId?
pageSize=pageSize&marker=marker&isAscendingOrder=ascendingOrder

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>caCertificateId</td>
<td>CertificateId</td>
<td>yes</td>
<td>The ID of the CA certificate. This operation will list all registered device certificates that were signed by this CA certificate.</td>
</tr>
<tr>
<td>pageSize</td>
<td>PageSize</td>
<td>no</td>
<td>The result page size.</td>
</tr>
<tr>
<td>marker</td>
<td>Marker</td>
<td>no</td>
<td>The marker for the next set of results.</td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>AscendingOrder</td>
<td>no</td>
<td>Specifies the order for results. If True, the results are returned in ascending order, based on the creation date.</td>
</tr>
</tbody>
</table>

**Response syntax:**

```json
Content-type: application/json
{
    "certificates": [
    {
        "certificateArn": "string",
        "certificateId": "string",
        "status": "string",
        "creationDate": "timestamp"
    },
    "nextMarker": "string"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificates</td>
<td>Certificates</td>
<td>no</td>
<td>The device certificates signed by the specified CA certificate.</td>
</tr>
<tr>
<td>nextMarker</td>
<td>Marker</td>
<td>no</td>
<td>The marker for the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

**Errors:**

895
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an
UpdateJobExecution request contains invalid status details. The message contains details about the
error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot list-certificates-by-ca 
   --ca-certificate-id <value> 
   [--page-size <value>] 
   [--marker <value>] 
   [--ascending-order | --no-ascending-order] 
   [--cli-input-json <value>] 
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "caCertificateId": "string",
   "pageSize": "integer",
   "marker": "string",
   "ascendingOrder": "boolean"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>caCertificateId</td>
<td>string</td>
<td>The ID of the CA certificate. This operation will list all registered device certificate that were signed by this CA certificate.</td>
</tr>
</tbody>
</table>
ListCertificatesByCA

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pageSize</td>
<td>integer, range 1-250</td>
<td>The result page size.</td>
</tr>
<tr>
<td>marker</td>
<td>string, pattern 0-2</td>
<td>The marker for the next set of results.</td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>boolean</td>
<td>Specifies the order for results. If True, results are returned in ascending order, based on creation date.</td>
</tr>
</tbody>
</table>

Output:

```json
{
  "certificates": [
    {
      "certificateArn": "string",
      "certificateId": "string",
      "status": "string",
      "creationDate": "timestamp"
    }
  ],
  "nextMarker": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificates</td>
<td>list, member: Certificate, java class: java.util.List</td>
<td>The device certificates signed by the specified CA certificate.</td>
</tr>
<tr>
<td>certificateArn</td>
<td>string</td>
<td>The ID of the certificate. (The last part of the certificate ARN contains the certificate ID.)</td>
</tr>
<tr>
<td>certificateId</td>
<td>string, length 1-64, pattern 0x[a-fA-F0-9]+</td>
<td>The status of the certificate.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the certificate.</td>
</tr>
</tbody>
</table>

- The status value REGISTER_INACTIVE is deprecated and should not be used.
- enum: ACTIVE | INACTIVE | REVOKED | PENDING_TRANSFER | REGISTER_INACTIVE | PENDING_ACTIVATION
ListIndices

Lists the search indices.

https

Request syntax:

GET /indices?nextToken=nextToken&maxResults=maxResults

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>QueryMaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>
Response syntax:

Content-type: application/json

```json
{
  "indexNames": [ "string"
  ],
  "nextToken": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>indexNames</td>
<td>IndexNamesList</td>
<td>no</td>
<td>The index names.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

```
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400
```

```
ThrottlingException

The rate exceeds the limit.

HTTP response code: 429
```

```
UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401
```

```
ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503
```

```
InternalFailureException

An unexpected error has occurred.

HTTP response code: 500
```

cli

Synopsis:
aws iot list-indices \
    [--next-token <value>] \
    [--max-results <value>] \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]

cli-input-json format:

```json
{
    "nextToken": "string",
    "maxResults": "integer"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>

Output:

```json
{
    "indexNames": [
        "string"
    ],
    "nextToken": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>indexNames</td>
<td>list</td>
<td>The index names.</td>
</tr>
<tr>
<td></td>
<td>member: IndexName</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

ListJobExecutionsForJob

Lists the job executions for a job.

https

Request syntax:

GET /jobs/jobId/things?status=status&maxResults=maxResults&nextToken=nextToken

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>JobId</td>
<td>yes</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td>status</td>
<td>JobExecutionStatus</td>
<td>no</td>
<td>The status of the job.</td>
</tr>
<tr>
<td>maxResults</td>
<td>LaserMaxResults</td>
<td>no</td>
<td>The maximum number of results to be returned per request.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token to retrieve the next set of results.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```
{
  "executionSummaries": [
    {
      "thingArn": "string",
      "jobExecutionSummary": {
        "status": "string",
        "queuedAt": "timestamp",
        "startedAt": "timestamp",
```
"lastUpdatedAt": "timestamp",
"executionNumber": "long"
} 
},
"nextToken": "string"
}

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>executionSummaries</td>
<td>JobExecutionSummaryForJobList</td>
<td>no</td>
<td>A list of job execution summaries.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

**Errors:**

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

**cli**

**Synopsis:**

```bash
aws iot list-job-executions-for-job \\   --job-id <value> \\
   [--status <value>] \\
   [--max-results <value>] \\
   [--next-token <value>] \\
   [--cli-input-json <value>] \\
```
ListJobExecutionsForJob

cli-input-json format:

```json
{
  "jobId": "string",
  "status": "string",
  "maxResults": "integer",
  "nextToken": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td>length-</td>
<td>max:64</td>
<td></td>
</tr>
<tr>
<td>min:1</td>
<td>pattern: [a-zA-Z0-9-]_+</td>
<td></td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the job.</td>
</tr>
<tr>
<td>enum:</td>
<td>QUEUED</td>
<td>IN_PROGRESS</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to be returned per request.</td>
</tr>
<tr>
<td>range- max:</td>
<td>250</td>
<td>min:1</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token to retrieve the next set of results.</td>
</tr>
</tbody>
</table>

Output:

```json
{
  "executionSummaries": [
    {
      "thingArn": "string",
      "jobExecutionSummary": {
        "status": "string",
        "queuedAt": "timestamp",
        "startedAt": "timestamp",
        "lastUpdatedAt": "timestamp",
        "executionNumber": "long"
      }
    },
    {
      "thingArn": "string",
      "jobExecutionSummary": {
        "status": "string",
        "queuedAt": "timestamp",
        "startedAt": "timestamp",
        "lastUpdatedAt": "timestamp",
        "executionNumber": "long"
      }
    }
  ],
  "nextToken": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>executionSummaries</td>
<td>list</td>
<td>A list of job execution summaries.</td>
</tr>
</tbody>
</table>
### ListJobExecutionsForJob

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingArn</td>
<td>string</td>
<td>The ARN of the thing on which the job execution is running.</td>
</tr>
<tr>
<td>jobExecutionSummary</td>
<td>JobExecutionSummary</td>
<td>Contains a subset of information about a job execution.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the job execution.</td>
</tr>
<tr>
<td>queuedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job execution was queued.</td>
</tr>
<tr>
<td>startedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job execution started.</td>
</tr>
<tr>
<td>lastUpdatedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job execution was last updated.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>long</td>
<td>A string (consisting of the digits &quot;0&quot; through &quot;9&quot;) which identifies this particular job execution on this particular device. It can be used later in commands which return or update job execution information.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

**Errors:**

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ResourceNotFoundException**
  
  The specified resource does not exist.

- **ThrottlingException**
  
  The rate exceeds the limit.

- **ServiceUnavailableException**
  
  The service is temporarily unavailable.
ListJobExecutionsForThing

Lists the job executions for the specified thing.

https

Request syntax:

GET /things/thingName/jobs?status=status&maxResults=maxResults&nextToken=nextToken

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The thing name.</td>
</tr>
<tr>
<td>status</td>
<td>JobExecutionStatus</td>
<td>no</td>
<td>An optional filter that lets you search for jobs that have the specified status.</td>
</tr>
<tr>
<td>maxResults</td>
<td>LaserMaxResults</td>
<td>no</td>
<td>The maximum number of results to be returned per request.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token to retrieve the next set of results.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{
  "executionSummaries": [
    {
      "jobId": "string",
      "jobExecutionSummary": {
        "status": "string",
        "queuedAt": "timestamp",
        "startedAt": "timestamp",
        "lastUpdatedAt": "timestamp",
        "executionNumber": "long"
      }
    }
  ],
  "nextToken": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>executionSummaries</td>
<td>JobExecutionSummaryForThingList</td>
<td>no</td>
<td>A list of job execution summaries.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results, or null if</td>
</tr>
</tbody>
</table>
ListJobExecutionsForThing

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
HTTP response code: 400

ResourceNotFoundException
The specified resource does not exist.
HTTP response code: 404

ThrottlingException
The rate exceeds the limit.
HTTP response code: 429

ServiceUnavailableException
The service is temporarily unavailable.
HTTP response code: 503

cli

Synopsis:

```
aws iot list-job-executions-for-thing \
  --thing-name <value> \
  [--status <value>] \
  [--max-results <value>] \
  [--next-token <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "thingName": "string",
  "status": "string",
  "maxResults": "integer",
  "nextToken": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The thing name.</td>
</tr>
</tbody>
</table>
### ListJobExecutionsForThing

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Length**: `max:128 min:1`  
  - **Pattern**: `[a-zA-Z0-9_:\-]+`  

- **Status**: `string`  
  - An optional filter that lets you search for jobs that have the specified status.  
  - **Enum**: QUEUED | IN_PROGRESS | SUCCEEDED | FAILED | REJECTED | REMOVED | CANCELED

- **MaxResults**: `integer`  
  - **Range**: `max:250 min:1`  
  - The maximum number of results to be returned per request.

- **NextToken**: `string`  
  - The token to retrieve the next set of results.

### Output:

```json
{
  "executionSummaries": [
    {
      "jobId": "string",
      "jobExecutionSummary": {
        "status": "string",
        "queuedAt": "timestamp",
        "startedAt": "timestamp",
        "lastUpdatedAt": "timestamp",
        "executionNumber": "long"
      }
    }
  ],
  "nextToken": "string"
}
```

### CLI output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>executionSummaries</td>
<td>list</td>
<td>A list of job execution summaries.</td>
</tr>
<tr>
<td>member:</td>
<td>JobExecutionSummaryForThing</td>
<td></td>
</tr>
<tr>
<td>java class:</td>
<td>java.util.List</td>
<td></td>
</tr>
<tr>
<td>jobld</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td>length- max:64 min:1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pattern:</td>
<td>[a-zA-Z0-9_:-]+</td>
<td></td>
</tr>
<tr>
<td>jobExecutionSummary</td>
<td>JobExecutionSummary</td>
<td>Contains a subset of information about a job execution.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the job execution.</td>
</tr>
</tbody>
</table>
### ListJobs

Lists jobs.

**https**

**Request syntax:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>Type</td>
<td>enum</td>
<td>Value: QUEUED</td>
</tr>
<tr>
<td>queuedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job execution was queued.</td>
</tr>
<tr>
<td>startedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job execution started.</td>
</tr>
<tr>
<td>lastUpdatedAt</td>
<td>timestamp</td>
<td>The time, in milliseconds since the epoch, when the job execution was last updated.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>long</td>
<td>A string (consisting of the digits &quot;0&quot; through &quot;9&quot;) which identifies this particular job execution on this particular device. It can be used later in commands which return or update job execution information.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

**ResourceNotFoundException**

The specified resource does not exist.

**ThrottlingException**

The rate exceeds the limit.

**ServiceUnavailableException**

The service is temporarily unavailable.
### GET /jobs?
status=status&targetSelection=targetSelection&maxResults=maxResults&nextToken=nextToken&thingGroupName=thingGroupName&thingGroupId=thingGroupId

#### URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>JobStatus</td>
<td>no</td>
<td>An optional filter that lets you search for jobs that have the specified status.</td>
</tr>
<tr>
<td>targetSelection</td>
<td>TargetSelection</td>
<td>no</td>
<td>Specifies whether the job will continue to run (CONTINUOUS), or will be complete after all those things specified as targets have completed the job (SNAPSHOT). If continuous, the job may also be run on a thing when a change is detected in a target. For example, a job will run on a thing when the thing is added to a target group, even after the job was completed by all things originally in the group.</td>
</tr>
<tr>
<td>maxResults</td>
<td>LaserMaxResults</td>
<td>no</td>
<td>The maximum number of results to return per request.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>thingGroupName</td>
<td>ThingGroupName</td>
<td>no</td>
<td>A filter that limits the returned jobs to those for the specified group.</td>
</tr>
<tr>
<td>thingGroupId</td>
<td>ThingGroupId</td>
<td>no</td>
<td>A filter that limits the returned jobs to those for the specified group.</td>
</tr>
</tbody>
</table>

#### Response syntax:

```
Content-type: application/json

{
    "jobs": [
        {
            "jobArn": "string",
            "jobId": "string",
            "thingGroupId": "string",
            ...
        }
    ]
}
```
"targetSelection": "string",
"status": "string",
"createdAt": "timestamp",
"lastUpdatedAt": "timestamp",
"completedAt": "timestamp"
},
"nextToken": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobs</td>
<td>JobSummaryList</td>
<td>no</td>
<td>A list of jobs.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

cli

Synopsis:

```
aws iot list-jobs \
  [--status <value>] \
  [--target-selection <value>] \
  [--max-results <value>] \
  [--next-token <value>] \
  [--thing-group-name <value>] \
```
## ListJobs

```
[ --thing-group-id <value> ] \n[ --cli-input-json <value> ] \n[ --generate-cli-skeleton ]
```

cli-input-json format:

```
{
  "status": "string",
  "targetSelection": "string",
  "maxResults": "integer",
  "nextToken": "string",
  "thingGroupName": "string",
  "thingGroupId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>string</td>
<td>An optional filter that lets you search for jobs that have the specified status.</td>
<td>enum: IN_PROGRESS</td>
</tr>
<tr>
<td>targetSelection</td>
<td>string</td>
<td>Specifies whether the job will continue to run (CONTINUOUS), or will be complete after all those things specified as targets have completed the job (SNAPSHOT). If continuous, the job may also be run on a thing when a change is detected in a target. For example, a job will run on a thing when the thing is added to a target group, even after the job was completed by all things originally in the group.</td>
<td>enum: CONTINUOUS</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return per request.</td>
<td>max:250 min:1</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token to retrieve the next set of results.</td>
<td></td>
</tr>
<tr>
<td>thingGroupName</td>
<td>string</td>
<td>A filter that limits the returned jobs to those for the specified group.</td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_]+</td>
</tr>
<tr>
<td>thingGroupId</td>
<td>string</td>
<td>A filter that limits the returned jobs to those for the specified group.</td>
<td>length- max:128 min:1</td>
</tr>
</tbody>
</table>
ListJobs

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>pattern: [a-zA-Z0-9-]+</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
  "jobs": [
    {
      "jobArn": "string",
      "jobId": "string",
      "thingGroupId": "string",
      "targetSelection": "string",
      "status": "string",
      "createdAt": "timestamp",
      "lastUpdatedAt": "timestamp",
      "completedAt": "timestamp"
    }
  ],
  "nextToken": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobs</td>
<td>list</td>
<td>A list of jobs.</td>
</tr>
<tr>
<td>jobArn</td>
<td>string</td>
<td>The job ARN.</td>
</tr>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td>length- max:64 min:1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pattern: [a-zA-Z0-9-]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>thingGroupId</td>
<td>string</td>
<td>The ID of the thing group.</td>
</tr>
<tr>
<td>length- max:128 min:1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pattern: [a-zA-Z0-9-]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>targetSelection</td>
<td>string</td>
<td>Specifies whether the job will continue to run (CONTINUOUS), or will be complete after all those things specified as targets have completed the job (SNAPSHOT). If continuous, the job may also be run on a thing when a change is detected in a target. For example, a job will run on a thing when the thing is added to a target group, even after the job was completed by all things originally in the group.</td>
</tr>
</tbody>
</table>
### ListOTAUpdates

### Description

Lists OTA updates.

### Request syntax:

```
GET /otaUpdates?maxResults=maxResults&nextToken=nextToken&otaUpdateStatus=otaUpdateStatus
```
URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td>nextPageToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token used to retrieve the next set of results.</td>
</tr>
<tr>
<td>otaUpdateStatus</td>
<td>OTAUpdateStatus</td>
<td>no</td>
<td>The OTA update job status.</td>
</tr>
</tbody>
</table>

Response syntax:

```json
Content-type: application/json

{
  "otaUpdates": [
    {
      "otaUpdateId": "string",
      "otaUpdateArn": "string",
      "creationDate": "timestamp"
    }
  ],
  "nextToken": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>otaUpdates</td>
<td>OTAUpdatesSummary</td>
<td>no</td>
<td>A list of OTA update jobs.</td>
</tr>
<tr>
<td>nextPageToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token to use to get the next set of results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401
InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

ServiceUnavailableException
The service is temporarily unavailable.
HTTP response code: 503

cli

Synopsis:

```
aws iot list-ota-updates \
  [--max-results <value>] \
  [--next-token <value>] \
  [--ota-update-status <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "maxResults": "integer",
  "nextToken": "string",
  "otaUpdateStatus": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td></td>
<td>range: max:250 min:1</td>
<td></td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>A token used to retrieve the next set of results.</td>
</tr>
<tr>
<td>otaUpdateStatus</td>
<td>string</td>
<td>The OTA update job status.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: CREATE_PENDING</td>
</tr>
</tbody>
</table>

Output:

```
{
  "otaUpdates": [ 
    {
      "otaUpdateId": "string",
      "otaUpdateArn": "string",
      "creationDate": "timestamp"
    }
  ],
}
```
"nextToken": "string"
}

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>otaUpdates</td>
<td>list</td>
<td>A list of OTA update jobs.</td>
</tr>
<tr>
<td>member: OTAUpdateSummary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>otaUpdateId</td>
<td>string</td>
<td>The OTA update ID.</td>
</tr>
<tr>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-_]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>otaUpdateArn</td>
<td>string</td>
<td>The OTA update ARN.</td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The date when the OTA update was created.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>A token to use to get the next set of results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

InternalFailureException

An unexpected error has occurred.

ServiceUnavailableException

The service is temporarily unavailable.

ListOutgoingCertificates

Lists certificates that are being transferred but not yet accepted.

https

Request syntax:

```
GET /certificates-out-going?
pageSize=pageSize&marker=marker&isAscendingOrder=ascendingOrder
```
URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pageSize</td>
<td>PageSize</td>
<td>no</td>
<td>The result page size.</td>
</tr>
<tr>
<td>marker</td>
<td>Marker</td>
<td>no</td>
<td>The marker for the next set of results.</td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>AscendingOrder</td>
<td>no</td>
<td>Specifies the order for results. If True, the results are returned in ascending order, based on the creation date.</td>
</tr>
</tbody>
</table>

Response syntax:

```
Content-type: application/json

{
  "outgoingCertificates": [
    {
      "certificateArn": "string",
      "certificateId": "string",
      "transferredTo": "string",
      "transferDate": "timestamp",
      "transferMessage": "string",
      "creationDate": "timestamp"
    }
  ],
  "nextMarker": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>outgoingCertificates</td>
<td>OutgoingCertificates</td>
<td>no</td>
<td>The certificates that are being transferred but not yet accepted.</td>
</tr>
<tr>
<td>nextMarker</td>
<td>Marker</td>
<td>no</td>
<td>The marker for the next set of results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429
UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot list-outgoing-certificates
   [--page-size <value>] \
   [--marker <value>] \
   [--ascending-order | --no-ascending-order] \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "pageSize": "integer",
   "marker": "string",
   "ascendingOrder": "boolean"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pageSize</td>
<td>integer</td>
<td>The result page size.</td>
</tr>
<tr>
<td></td>
<td>range- max:250 min:1</td>
<td></td>
</tr>
<tr>
<td>marker</td>
<td>string</td>
<td>The marker for the next set of results.</td>
</tr>
<tr>
<td></td>
<td>pattern: [A-Za-z0-9+/]+={0,2}</td>
<td></td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>boolean</td>
<td>Specifies the order for results. If True, the results are returned in ascending order, based on the creation date.</td>
</tr>
</tbody>
</table>

Output:

```
{
   "outgoingCertificates": [
      {
         "certificateArn": "string",
```
"certificateId": "string",
"transferredTo": "string",
"transferDate": "timestamp",
"transferMessage": "string",
"creationDate": "timestamp"
},
"nextMarker": "string"
}

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>outgoingCertificates</td>
<td>list</td>
<td>The certificates that are being transferred but not yet accepted.</td>
</tr>
<tr>
<td></td>
<td>member:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OutgoingCertificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class:</td>
<td>java.util.List</td>
</tr>
<tr>
<td>certificateArn</td>
<td>string</td>
<td>The certificate ARN.</td>
</tr>
<tr>
<td>certificateId</td>
<td>string</td>
<td>The certificate ID.</td>
</tr>
<tr>
<td></td>
<td>length-</td>
<td>max:64 min:64</td>
</tr>
<tr>
<td></td>
<td>pattern:</td>
<td>(0x)?[a-fA-F0-9]+</td>
</tr>
<tr>
<td>transferredTo</td>
<td>string</td>
<td>The AWS account to which the transfer was made.</td>
</tr>
<tr>
<td></td>
<td>length-</td>
<td>max:12 min:12</td>
</tr>
<tr>
<td></td>
<td>pattern:</td>
<td>[0-9]+</td>
</tr>
<tr>
<td>transferDate</td>
<td>timestamp</td>
<td>The date the transfer was initiated.</td>
</tr>
<tr>
<td>transferMessage</td>
<td>string</td>
<td>The transfer message.</td>
</tr>
<tr>
<td></td>
<td>length-</td>
<td>max:128</td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The certificate creation date.</td>
</tr>
<tr>
<td>nextMarker</td>
<td>string</td>
<td>The marker for the next set of results.</td>
</tr>
<tr>
<td></td>
<td>pattern:</td>
<td>[A-Za-z0-9+/]+={0,2}</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.
ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

ListPolicies

Lists your policies.

https

Request syntax:

GET /policies?marker=marker&pageSize=pageSize&isAscendingOrder=ascendingOrder

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>marker</td>
<td>Marker</td>
<td>no</td>
<td>The marker for the next set of results.</td>
</tr>
<tr>
<td>pageSize</td>
<td>PageSize</td>
<td>no</td>
<td>The result page size.</td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>AscendingOrder</td>
<td>no</td>
<td>Specifies the order for results. If true, the results are returned in ascending creation order.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```
{
  "policies": [
    {
      "policyName": "string",
      "policyArn": "string"
    }
  ],
  "nextMarker": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policies</td>
<td>Policies</td>
<td>no</td>
<td>The descriptions of the policies.</td>
</tr>
</tbody>
</table>
ListPolicies

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextMarker</td>
<td>Marker</td>
<td>no</td>
<td>The marker for the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot list-policies
   [--marker <value>] 
   [--page-size <value>] 
   [--ascending-order | --no-ascending-order] 
   [--cli-input-json <value>] 
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "marker": "string",
   "pageSize": "integer",
   "ascendingOrder": "boolean"
}
```
cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>marker</td>
<td>string</td>
<td>The marker for the next set of results.</td>
</tr>
<tr>
<td></td>
<td>pattern</td>
<td>[A-Za-z0-9+/]+={0,2}</td>
</tr>
<tr>
<td>pageSize</td>
<td>integer</td>
<td>The result page size.</td>
</tr>
<tr>
<td></td>
<td>range</td>
<td>max:250 min:1</td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>boolean</td>
<td>Specifies the order for results. If true, the results are returned in ascending creation order.</td>
</tr>
</tbody>
</table>

Output:

```json
{
  "policies": [
    {
      "policyName": "string",
      "policyArn": "string"
    }
  ],
  "nextMarker": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policies</td>
<td>list</td>
<td>The descriptions of the policies.</td>
</tr>
<tr>
<td></td>
<td>member</td>
<td>Policy</td>
</tr>
<tr>
<td></td>
<td>java</td>
<td>class: java.util.List</td>
</tr>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
<tr>
<td></td>
<td>length</td>
<td>max:128 min:1</td>
</tr>
<tr>
<td></td>
<td>pattern</td>
<td>[w+=,.@-]+</td>
</tr>
<tr>
<td>policyArn</td>
<td>string</td>
<td>The policy ARN.</td>
</tr>
<tr>
<td>nextMarker</td>
<td>string</td>
<td>The marker for the next set of results, or null if there are no additional results.</td>
</tr>
<tr>
<td></td>
<td>pattern</td>
<td>[A-Za-z0-9+/]+={0,2}</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

ListPolicyPrincipals

List the principals associated with the specified policy.

Note: This API is deprecated. Please use ListTargetsForPolicy instead.

https

Request syntax:

GET /policy-principals?marker=marker&pageSize=pageSize&isAscendingOrder=ascendingOrder
x-amzn-iot-policy: policyName

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>yes</td>
<td>The policy name.</td>
</tr>
<tr>
<td>marker</td>
<td>Marker</td>
<td>no</td>
<td>The marker for the next set of results.</td>
</tr>
<tr>
<td>pageSize</td>
<td>PageSize</td>
<td>no</td>
<td>The result page size.</td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>AscendingOrder</td>
<td>no</td>
<td>Specifies the order for results. If true, the results are returned in ascending creation order.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{
    "principals": [
        "string"
    ],
    "nextMarker": "string"
Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>principals</td>
<td>Principals</td>
<td>no</td>
<td>The descriptions of the principals.</td>
</tr>
<tr>
<td>nextMarker</td>
<td>Marker</td>
<td>no</td>
<td>The marker for the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```bash
aws iot list-policy-principals \
    --policy-name <value> \
    [--marker <value>] \
```
[--page-size <value>] \
[--ascending-order | --no-ascending-order] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]

cli-input-json format:

```
{
  "policyName": "string",
  "marker": "string",
  "pageSize": "integer",
  "ascendingOrder": "boolean"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w+=,.@-]+</td>
<td></td>
</tr>
<tr>
<td>marker</td>
<td>string</td>
<td>The marker for the next set of results.</td>
</tr>
<tr>
<td></td>
<td>pattern: [A-Za-z0-9+/]+={0,2}</td>
<td></td>
</tr>
<tr>
<td>pageSize</td>
<td>integer</td>
<td>The result page size.</td>
</tr>
<tr>
<td></td>
<td>range- max:250 min:1</td>
<td></td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>boolean</td>
<td>Specifies the order for results. If true, the results are returned in</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ascending creation order.</td>
</tr>
</tbody>
</table>

Output:

```
{
  "principals": [  
    "string"
  ],
  "nextMarker": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>principals</td>
<td>list</td>
<td>The descriptions of the principals.</td>
</tr>
<tr>
<td></td>
<td>member: PrincipalArn</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>nextMarker</td>
<td>string</td>
<td>The marker for the next set of results, or null if there are no additional</td>
</tr>
<tr>
<td></td>
<td>pattern: [A-Za-z0-9+/]+={0,2}</td>
<td>results.</td>
</tr>
</tbody>
</table>
ListPolicyVersions

Lists the versions of the specified policy and identifies the default version.

https

Request syntax:

GET /policies/policyName/version

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>yes</td>
<td>The policy name.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```json
{
   "policyVersions": [
   {
      "versionId": "string",
      "isDefaultVersion": "boolean",
      "createDate": "timestamp"
   }
   ]
}
```
Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyVersions</td>
<td>PolicyVersions</td>
<td>no</td>
<td>The policy versions.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException
The specified resource does not exist.
HTTP response code: 404

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
HTTP response code: 400

ThrottlingException
The rate exceeds the limit.
HTTP response code: 429

UnauthorizedException
You are not authorized to perform this operation.
HTTP response code: 401

ServiceUnavailableException
The service is temporarily unavailable.
HTTP response code: 503

InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

cli

Synopsis:

```
aws iot list-policy-versions
   --policy-name <value>
   [--cli-input-json <value>]
   [--generate-cli-skeleton]
```

cli-input-json format:
```
{
  "policyName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w+=,.@-]+</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```
{
  "policyVersions": [
    {
      "versionId": "string",
      "isDefaultVersion": "boolean",
      "createDate": "timestamp"
    }
  ]
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyVersions</td>
<td>list</td>
<td>The policy versions.</td>
</tr>
<tr>
<td></td>
<td>member: PolicyVersion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>versionId</td>
<td>string</td>
<td>The policy version ID.</td>
</tr>
<tr>
<td></td>
<td>pattern: [0-9]+</td>
<td></td>
</tr>
<tr>
<td>isDefaultVersion</td>
<td>boolean</td>
<td>Specifies whether the policy version is the default.</td>
</tr>
<tr>
<td>createDate</td>
<td>timestamp</td>
<td>The date and time the policy was created.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException

The specified resource does not exist.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
ListPrincipalPolicies

Lists the policies attached to the specified principal. If you use an Cognito identity, the ID must be in AmazonCognito Identity format.

**Note:** This API is deprecated. Please use ListAttachedPolicies instead.

**https**

**Request syntax:**

```
GET /principal-policies?marker=marker&pageSize=pageSize&isAscendingOrder=ascendingOrder
x-amzn-iot-principal: principal
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>principal</td>
<td>Principal</td>
<td>yes</td>
<td>The principal.</td>
</tr>
<tr>
<td>marker</td>
<td>Marker</td>
<td>no</td>
<td>The marker for the next set of results.</td>
</tr>
<tr>
<td>pageSize</td>
<td>PageSize</td>
<td>no</td>
<td>The result page size.</td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>AscendingOrder</td>
<td>no</td>
<td>Specifies the order for results. If true, results are returned in ascending creation order.</td>
</tr>
</tbody>
</table>

**Response syntax:**

```
Content-type: application/json

{
  "policies": [
    {
      "policyName": "string",
    }
  ]
```
"policyArn": "string"
},
"nextMarker": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policies</td>
<td>Policies</td>
<td>no</td>
<td>The policies.</td>
</tr>
<tr>
<td>nextMarker</td>
<td>Marker</td>
<td>no</td>
<td>The marker for the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException
The specified resource does not exist.
HTTP response code: 404

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
HTTP response code: 400

ThrottlingException
The rate exceeds the limit.
HTTP response code: 429

UnauthorizedException
You are not authorized to perform this operation.
HTTP response code: 401

ServiceUnavailableException
The service is temporarily unavailable.
HTTP response code: 503

InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

cli

Synopsis:
aws iot list-principal-policies \
   --principal <value> \ 
   [--marker <value>] \ 
   [--page-size <value>] \ 
   [--ascending-order | --no-ascending-order] \ 
   [--cli-input-json <value>] \ 
   [--generate-cli-skeleton]

cli-input-json format:

```
{
   "principal": "string",
   "marker": "string",
   "pageSize": "integer",
   "ascendingOrder": "boolean"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>principal</td>
<td>string</td>
<td>The principal.</td>
</tr>
<tr>
<td>marker</td>
<td>string</td>
<td>The marker for the next set of results.</td>
</tr>
<tr>
<td>pattern</td>
<td></td>
<td>pattern: [A-Za-z0-9+/]+={0,2}</td>
</tr>
<tr>
<td>pageSize</td>
<td>integer</td>
<td>The result page size.</td>
</tr>
<tr>
<td>range- max:</td>
<td></td>
<td>max:250 min:1</td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>boolean</td>
<td>Specifies the order for results. If true, results are returned in ascending creation order.</td>
</tr>
</tbody>
</table>

Output:

```
{
   "policies": [
   {
      "policyName": "string",
      "policyArn": "string"
   }
  ],
  "nextMarker": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policies</td>
<td>list</td>
<td>The policies.</td>
</tr>
<tr>
<td></td>
<td>member: Policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
</tbody>
</table>
### ListPrincipalThings

Lists the things associated with the specified principal.

**https**

**Request syntax:**

```
GET /principals/things?maxResults=maxResults&nextToken=nextToken
x-amzn-principal: principal
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token to retrieve the next set of results.</td>
</tr>
</tbody>
</table>
ListPrincipalThings

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxResults</td>
<td>RegistryMaxResults</td>
<td>no</td>
<td>The maximum number of results to return in this operation.</td>
</tr>
<tr>
<td>principal</td>
<td>Principal</td>
<td>yes</td>
<td>The principal.</td>
</tr>
</tbody>
</table>

Response syntax:

```json
Content-type: application/json
{
   "things": [
      "string"
   ],
   "nextToken": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>things</td>
<td>ThingNameList</td>
<td>no</td>
<td>The things.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503
InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

ResourceNotFoundException
The specified resource does not exist.
HTTP response code: 404

cli

Synopsis:

```
aws iot list-principal-things \
[--next-token <value>] \
[--max-results <value>] \
--principal <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "nextToken": "string",
   "maxResults": "integer",
   "principal": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return in this operation.</td>
</tr>
<tr>
<td></td>
<td>range: max:250 min:1</td>
<td></td>
</tr>
<tr>
<td>principal</td>
<td>string</td>
<td>The principal.</td>
</tr>
</tbody>
</table>

Output:

```
{
   "things": [
      "string"
   ],
   "nextToken": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>things</td>
<td>list</td>
<td>The things.</td>
</tr>
</tbody>
</table>
ListRoleAliases

Lists the role aliases registered in your account.

https

Request syntax:

```
GET /role-aliases?pageSize=pageSize&marker=marker&isAscendingOrder=ascendingOrder
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pageSize</td>
<td>PageSize</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td>marker</td>
<td>Marker</td>
<td>no</td>
<td>A marker used to get the next set of results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

ResourceNotFoundException

The specified resource does not exist.
ListRoleAliases

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ascendingOrder</td>
<td>AscendingOrder</td>
<td>no</td>
<td>Return the list of role aliases in ascending alphabetical order.</td>
</tr>
</tbody>
</table>

**Response syntax:**

```
Content-type: application/json

{
  "roleAliases": ["string"],
  "nextMarker": "string"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleAliases</td>
<td>RoleAliases</td>
<td>no</td>
<td>The role aliases.</td>
</tr>
<tr>
<td>nextMarker</td>
<td>Marker</td>
<td>no</td>
<td>A marker used to get the next set of results.</td>
</tr>
</tbody>
</table>

**Errors:**

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

  - HTTP response code: 400

- **ThrottlingException**
  
  The rate exceeds the limit.

  - HTTP response code: 429

- **UnauthorizedException**
  
  You are not authorized to perform this operation.

  - HTTP response code: 401

- **ServiceUnavailableException**
  
  The service is temporarily unavailable.

  - HTTP response code: 503

- **InternalFailureException**
  
  An unexpected error has occurred.

  - HTTP response code: 500
cli

Synopsis:

```
aws iot list-role-aliases \
  [--page-size <value>] \
  [--marker <value>] \
  [--ascending-order | --no-ascending-order] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "pageSize": "integer",
  "marker": "string",
  "ascendingOrder": "boolean"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pageSize</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td></td>
<td>range: max:250 min:1</td>
<td></td>
</tr>
<tr>
<td>marker</td>
<td>string</td>
<td>A marker used to get the next set of results.</td>
</tr>
<tr>
<td></td>
<td>pattern: [A-Za-z0-9+/]+={0,2}</td>
<td></td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>boolean</td>
<td>Return the list of role aliases in ascending alphabetical order.</td>
</tr>
</tbody>
</table>

Output:

```
{
  "roleAliases": [
    "String"
  ],
  "nextMarker": "String"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleAliases</td>
<td>list</td>
<td>The role aliases.</td>
</tr>
<tr>
<td></td>
<td>member: RoleAlias</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>nextMarker</td>
<td>string</td>
<td>A marker used to get the next set of results.</td>
</tr>
<tr>
<td></td>
<td>pattern: [A-Za-z0-9+/]+={0,2}</td>
<td></td>
</tr>
</tbody>
</table>
Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

ListScheduledAudits

Lists all of your scheduled audits.

https

Request syntax:

GET /audit/scheduledaudits?maxResults=maxResults&nextToken=nextToken

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time. The default is 25.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{   "scheduledAudits": [   {   "scheduledAuditName": "string",   "scheduledAuditArn": "string",   "scheduledAuditStatus": "scheduledAuditStatus"   },   ...  ]   }
"frequency": "string",
"dayOfMonth": "string",
"dayOfWeek": "string"
},
"nextToken": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAudits</td>
<td>ScheduledAuditMetadataList</td>
<td>no</td>
<td>The list of scheduled audits.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot list-scheduled-audits
    [--next-token <value>]
    [--max-results <value>]
    [--cli-input-json <value>]
    [--generate-cli-skeleton]
```

cli-input-json format:

```
{
    "nextToken": "string",
```
"maxResults": "integer"
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time. The default is 25.</td>
</tr>
<tr>
<td></td>
<td>range- max:250 min:1</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```
{
    "scheduledAudits": [
        {
            "scheduledAuditName": "string",
            "scheduledAuditArn": "string",
            "frequency": "string",
            "dayOfMonth": "string",
            "dayOfWeek": "string"
        }
    ],
    "nextToken": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAudits</td>
<td>list</td>
<td>The list of scheduled audits.</td>
</tr>
<tr>
<td></td>
<td>member:</td>
<td>ScheduledAuditMetadata</td>
</tr>
<tr>
<td></td>
<td>java class:</td>
<td>java.util.List</td>
</tr>
<tr>
<td>scheduledAuditName</td>
<td>string</td>
<td>The name of the scheduled audit.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>scheduledAuditArn</td>
<td>string</td>
<td>The ARN of the scheduled audit.</td>
</tr>
<tr>
<td>frequency</td>
<td>string</td>
<td>How often the scheduled audit takes place.</td>
</tr>
<tr>
<td></td>
<td>enum: DAILY</td>
<td>WEEKLY</td>
</tr>
<tr>
<td>dayOfMonth</td>
<td>string</td>
<td>The day of the month on which the scheduled audit is run</td>
</tr>
<tr>
<td></td>
<td>pattern: ^([1-9]</td>
<td>1[2][0-9]</td>
</tr>
</tbody>
</table>
ListSecurityProfiles

Lists the Device Defender security profiles you have created. You can use filters to list only those security profiles associated with a thing group or only those associated with your account.

**https**

**Request syntax:**

```
GET /security-profiles?maxResults=maxResults&nextToken=nextToken
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>

**Errors:**

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.
Response syntax:

```
Content-type: application/json

{
   "securityProfileIdentifiers": [
      {
         "name": "string",
         "arn": "string"
      }
   ],
   "nextToken": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileIdentifiers</td>
<td>SecurityProfileIdentifiers</td>
<td>no</td>
<td>A list of security profile identifiers (names and ARNs).</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot list-security-profiles \
    [--next-token <value>] \
    [--max-results <value>] \
    [--cli-input-json <value>] \
```
cli-input-json format:

```json
{
    "nextToken": "string",
    "maxResults": "integer"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>

Output:

```json
{
    "securityProfileIdentifiers": [
        {
            "name": "string",
            "arn": "string"
        }
    ],
    "nextToken": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileIdentifiers</td>
<td>list</td>
<td>A list of security profile identifiers (names and ARNs).</td>
</tr>
<tr>
<td></td>
<td>member:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SecurityProfileIdentifier</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class:</td>
<td>java.util.List</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the security profile.</td>
</tr>
<tr>
<td></td>
<td>length:</td>
<td>max:128 min:1</td>
</tr>
<tr>
<td></td>
<td>pattern:</td>
<td>[a-zA-Z0-9:-_]+</td>
</tr>
<tr>
<td>arn</td>
<td>string</td>
<td>The ARN of the security profile.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>A token that can be used to retrieve the next set of results, or null if</td>
</tr>
<tr>
<td></td>
<td></td>
<td>there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

ListSecurityProfilesForTarget

Lists the Device Defender security profiles attached to a target (thing group).

https

Request syntax:

GET /security-profiles-for-target?
maxResults=maxResults&nextToken=nextToken&recursive=recursive&securityProfileTargetArn=securityProfileTargetArn

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td>recursive</td>
<td>Recursive</td>
<td>no</td>
<td>If true, return child groups as well.</td>
</tr>
<tr>
<td>securityProfileTargetArn</td>
<td>SecurityProfileTargetArn</td>
<td>yes</td>
<td>The ARN of the target (thing group) whose attached security profiles you want to get.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```json
{
    "securityProfileTargetMappings": [
        {
            "securityProfileIdentifier": {
                "name": "string",
                "arn": "string"
            }
        }
    ]
}
```
"target": {   "arn": "string" }
}
], "nextToken": "string" 

### Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileTargetMappings</td>
<td>SecurityProfileTargetMappings</td>
<td>no</td>
<td>A list of security profiles and their associated targets.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

### Errors:

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an `UpdateJobExecution` request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404

### Synopsis:

```bash
aws iot list-security-profiles-for-target
   [--next-token <value>] 
   [--max-results <value>] 
   [--recursive | --no-recursive] 
   --security-profile-target-arn <value> 
   [--cli-input-json <value>] 
```
cli-input-json format:

```
{
  "nextToken": "string",
  "maxResults": "integer",
  "recursive": "boolean",
  "securityProfileTargetArn": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td>recursive</td>
<td>boolean</td>
<td>If true, return child groups as well.</td>
</tr>
<tr>
<td>securityProfileTargetArn</td>
<td>string</td>
<td>The ARN of the target (thing group) whose attached security profiles you want to get.</td>
</tr>
</tbody>
</table>

Output:

```
{
  "securityProfileTargetMappings": [
    {
      "securityProfileIdentifier": {
        "name": "string",
        "arn": "string"
      },
      "target": {
        "arn": "string"
      }
    },
    {
      "nextToken": "string"
    }
  ]
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileTargetMappings</td>
<td>list member: SecurityProfileTargetMapping java class: java.util.List</td>
<td>A list of security profiles and their associated targets.</td>
</tr>
<tr>
<td>securityProfileIdentifier</td>
<td>SecurityProfileIdentifier</td>
<td>Information that identifies the security profile.</td>
</tr>
</tbody>
</table>
ListStreams

Lists all of the streams in your AWS account.

**https**

**Request syntax:**

```
GET /streams?maxResults=maxResults&nextToken=nextToken&isAscendingOrder=ascendingOrder
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at a time.</td>
</tr>
</tbody>
</table>

**Errors:**

- **InvalidRequestException**
  
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ThrottlingException**
  
The rate exceeds the limit.

- **InternalFailureException**
  
  An unexpected error has occurred.

- **ResourceNotFoundException**
  
The specified resource does not exist.

---

### Table

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the security profile.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>arn</td>
<td>string</td>
<td>The ARN of the security profile.</td>
</tr>
<tr>
<td>target</td>
<td>SecurityProfileTarget</td>
<td>Information about the target (thing group) associated with the security profile.</td>
</tr>
<tr>
<td>arn</td>
<td>string</td>
<td>The ARN of the security profile.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>
ListStreams

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token used to get the next set of results.</td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>AscendingOrder</td>
<td>no</td>
<td>Set to true to return the list of streams in ascending order.</td>
</tr>
</tbody>
</table>

Response syntax:

```json
Content-type: application/json

{
  "streams": [
    {
      "streamId": "string",
      "streamArn": "string",
      "streamVersion": "integer",
      "description": "string"
    }
  ],
  "nextToken": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streams</td>
<td>StreamsSummary</td>
<td>no</td>
<td>A list of streams.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token used to get the next set of results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503
InternalFailureException

An unexpected error has occurred.
HTTP response code: 500

cli

Synopsis:

```bash
aws iot list-streams \
    [--max-results <value>] \
    [--next-token <value>] \
    [--ascending-order | --no-ascending-order] \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
    "maxResults": "integer",
    "nextToken": "string",
    "ascendingOrder": "boolean"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at a time.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>A token used to get the next set of results.</td>
</tr>
<tr>
<td>ascendingOrder</td>
<td>boolean</td>
<td>Set to true to return the list of streams in ascending order.</td>
</tr>
</tbody>
</table>

Output:

```json
{
    "streams": [
        {
            "streamId": "string",
            "streamArn": "string",
            "streamVersion": "integer",
            "description": "string"
        }
    ],
    "nextToken": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streams</td>
<td>list</td>
<td>A list of streams.</td>
</tr>
</tbody>
</table>
ListTargetsForPolicy

List targets for the specified policy.

https

Request syntax:

```
POST /policy-targets/policyName?marker=marker&pageSize=pageSize
```
### ListTargetsForPolicy

#### URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>yes</td>
<td>The policy name.</td>
</tr>
<tr>
<td>marker</td>
<td>Marker</td>
<td>no</td>
<td>A marker used to get the next set of results.</td>
</tr>
<tr>
<td>pageSize</td>
<td>PageSize</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>

#### Response syntax:

```json
Content-type: application/json
{
  "targets": [
    "string"
  ],
  "nextMarker": "string"
}
```

#### Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targets</td>
<td>PolicyTargets</td>
<td>no</td>
<td>The policy targets.</td>
</tr>
<tr>
<td>nextMarker</td>
<td>Marker</td>
<td>no</td>
<td>A marker used to get the next set of results.</td>
</tr>
</tbody>
</table>

#### Errors:

- **ResourceNotFoundException**
  
  The specified resource does not exist.
  
  HTTP response code: 404

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  
  HTTP response code: 400

- **ThrottlingException**
  
  The rate exceeds the limit.
  
  HTTP response code: 429

- **UnauthorizedException**
  
  You are not authorized to perform this operation.
  
  HTTP response code: 401
ServiceUnavailableException
The service is temporarily unavailable.
HTTP response code: 503

InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

LimitExceededException
A limit has been exceeded.
HTTP response code: 410

cli

Synopsis:

```
aws iot list-targets-for-policy \
  --policy-name <value> \
  [--marker <value>] \
  [--page-size <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "policyName": "string",
  "marker": "string",
  "pageSize": "integer"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
<tr>
<td></td>
<td>length: max:128</td>
<td>min:1 pattern: [w+=,.@-]+</td>
</tr>
<tr>
<td>marker</td>
<td>string</td>
<td>A marker used to get the next set of results.</td>
</tr>
<tr>
<td></td>
<td>pattern: [A-Za-z0-9+/]{0,2}</td>
<td></td>
</tr>
<tr>
<td>pageSize</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td></td>
<td>range: max:250 min:1</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```
{
```

952
"targets": [ "string" ],
"nextMarker": "string" }

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targets</td>
<td>list</td>
<td>The policy targets.</td>
</tr>
<tr>
<td></td>
<td>member: PolicyTarget java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>nextMarker</td>
<td>string</td>
<td>A marker used to get the next set of results.</td>
</tr>
<tr>
<td></td>
<td>pattern: [A-Za-z0-9+/-]=?{0,2}</td>
<td></td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException

The specified resource does not exist.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

LimitExceeded Exception

A limit has been exceeded.

ListTargetsForSecurityProfile

Lists the targets (thing groups) associated with a given Device Defender security profile.

https

Request syntax:
ListTargetsForSecurityProfile

GET /security-profiles/securityProfileName/targets?
maxResults=maxResults&nextToken=nextToken

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>yes</td>
<td>The security profile.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>

**Response syntax:**

```json
Content-type: application/json

{
  "securityProfileTargets": [
    {
      "arn": "string"
    },
    "nextToken": "string"
  ]
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileTargets</td>
<td>SecurityProfileTargets</td>
<td>no</td>
<td>The thing groups to which the security profile is attached.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

**Errors:**

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404
ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot list-targets-for-security-profile
   --security-profile-name <value>
   [--next-token <value>]
   [--max-results <value>]
   [--cli-input-json <value>]
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "securityProfileName": "string",
   "nextToken": "string",
   "maxResults": "integer"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The security profile.</td>
</tr>
<tr>
<td></td>
<td>length</td>
<td>max:128 min:1</td>
</tr>
<tr>
<td></td>
<td>pattern</td>
<td>[a-zA-Z0-9:-_]+</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td></td>
<td>range</td>
<td>max:250 min:1</td>
</tr>
</tbody>
</table>

Output:

```
{
   "securityProfileTargets": [
      {
         "arn": "string"
      },
   "nextToken": "string"
}
```
### cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileTargets</td>
<td>list member: SecurityProfileTarget java class: java.util.List</td>
<td>The thing groups to which the security profile is attached.</td>
</tr>
<tr>
<td>arn</td>
<td>string</td>
<td>The ARN of the security profile.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

### Errors:

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

**ResourceNotFoundException**

The specified resource does not exist.

**ThrottlingException**

The rate exceeds the limit.

**InternalFailureException**

An unexpected error has occurred.

---

### ListThingGroups

List the thing groups in your account.

**https**

#### Request syntax:

```text
GET /thing-groups?maxResults=maxResults&nextToken=nextToken&parentGroup=parentGroup&namePrefixFilter=namePrefixFilter&recursive=recursive&thingGroupName=thingGroupName&rootOnly=rootOnly
```

#### URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>RegistryMaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>
### ListThingGroups

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>parentGroup</td>
<td>ThingGroupName</td>
<td>no</td>
<td>A filter that limits the results to those with the specified parent group.</td>
</tr>
<tr>
<td>namePrefixFilter</td>
<td>ThingGroupName</td>
<td>no</td>
<td>A filter that limits the results to those with the specified name prefix.</td>
</tr>
<tr>
<td>recursive</td>
<td>RecursiveWithoutDefault</td>
<td>no</td>
<td>If true, return child groups as well.</td>
</tr>
<tr>
<td>thingGroupName</td>
<td>ThingGroupName</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>rootOnly</td>
<td>RootOnly</td>
<td>no</td>
<td></td>
</tr>
</tbody>
</table>

**Response syntax:**

```
Content-type: application/json

{
  "thingGroups": [
    {
      "groupName": "string",
      "groupArn": "string"
    },
    "nextToken": "string"
  ]
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroups</td>
<td>ThingGroupNameAndArnList</td>
<td>no</td>
<td>The thing groups.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**InternalFailureException**

An unexpected error has occurred.
HTTP response code: 500
ResourceNotFoundException
The specified resource does not exist.

HTTP response code: 404
ThrottlingException
The rate exceeds the limit.

HTTP response code: 429

cli

Synopsis:

```
aws iot list-thing-groups \
   [--next-token <value>] \
   [--max-results <value>] \
   [--parent-group <value>] \
   [--name-prefix-filter <value>] \
   [--recursive | --no-recursive] \
   [--thing-group-name <value>] \
   [--root-only | --no-root-only] \n   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "nextToken": "string",
   "maxResults": "integer",
   "parentGroup": "string",
   "namePrefixFilter": "string",
   "recursive": "boolean",
   "thingGroupName": "string",
   "rootOnly": "boolean"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>Range: max: 250 min: 1</td>
</tr>
<tr>
<td>parentGroup</td>
<td>string</td>
<td>A filter that limits the results to those with the specified parent group.</td>
</tr>
<tr>
<td>namePrefixFilter</td>
<td>string</td>
<td>A filter that limits the results to those with the specified name prefix.</td>
</tr>
</tbody>
</table>
ListThingGroups

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>recursive</td>
<td>boolean</td>
<td>If true, return child groups as well.</td>
</tr>
<tr>
<td>thingGroupName</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td>The group name.</td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td>The group ARN.</td>
</tr>
<tr>
<td>rootOnly</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
   "thingGroups": [
      {
         "groupName": "string",
         "groupArn": "string"
      }
   ],
   "nextToken": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroups</td>
<td>list</td>
<td>The thing groups.</td>
</tr>
<tr>
<td></td>
<td>member: GroupNameAndArn</td>
<td>The thing groups.</td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td>The thing groups.</td>
</tr>
<tr>
<td>groupName</td>
<td>string</td>
<td>The group name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td>The group name.</td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td>The group ARN.</td>
</tr>
<tr>
<td>groupArn</td>
<td>string</td>
<td>The group ARN.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

**InternalFailureException**

An unexpected error has occurred.
ResourceNotFoundException
The specified resource does not exist.
ThrottlingException
The rate exceeds the limit.

ListThingGroupsForThing

List the thing groups to which the specified thing belongs.

https

Request syntax:

GET /things/thingName/thing-groups?maxResults=maxResults&nextToken=nextToken

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The thing name.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>RegistryMaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```json
{
  "thingGroups": [
    {
      "groupName": "string",
      "groupArn": "string"
    }
  ],
  "nextToken": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroups</td>
<td>ThingGroupNameAndArnList</td>
<td></td>
<td>The thing groups.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>
Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

cli

Synopsis:

```
aws iot  list-thing-groups-for-thing \
    --thing-name <value> \ 
    [--next-token <value>] \ 
    [--max-results <value>] \ 
    [--cli-input-json <value>] \ 
    [--generate-cli-skeleton]
```

cli-input-json format:

```
{
    "thingName": "string",
    "nextToken": "string",
    "maxResults": "integer"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The thing name.</td>
</tr>
<tr>
<td></td>
<td>length-</td>
<td>max:128 min:1</td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:-_]+</td>
<td></td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token to retrieve the next set of results.</td>
</tr>
</tbody>
</table>
ListThingGroupsForThing

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td></td>
<td>range: max:250 min:1</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
  "thingGroups": [
    {
      "groupName": "string",
      "groupArn": "string"
    },
    {
      "groupName": "string",
      "groupArn": "string"
    }
  ],
  "nextToken": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroups</td>
<td>list</td>
<td>The thing groups.</td>
</tr>
<tr>
<td></td>
<td>member: GroupNameAndArn</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>groupName</td>
<td>string</td>
<td>The group name.</td>
</tr>
<tr>
<td></td>
<td>length: max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>groupArn</td>
<td>string</td>
<td>The group ARN.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

InternalFailureException

An unexpected error has occurred.

ResourceNotFoundException

The specified resource does not exist.

ThrottlingException

The rate exceeds the limit.
ListThingPrincipals

Lists the principals associated with the specified thing.

https

Request syntax:

GET /things/thingName/principals

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{  
  "principals": [  
    "string"  
  ]  
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>principals</td>
<td>Principals</td>
<td>no</td>
<td>The principals associated with the thing.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401
ServiceUnavailableException
  The service is temporarily unavailable.
  HTTP response code: 503

InternalFailureException
  An unexpected error has occurred.
  HTTP response code: 500

ResourceNotFoundException
  The specified resource does not exist.
  HTTP response code: 404

cli

Synopsis:

```
aws iot list-thing-principals \
  --thing-name <value>  \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "thingName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing.</td>
</tr>
</tbody>
</table>

Output:

```
{
  "principals": [
    "string"
  ]
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>principals</td>
<td>list</td>
<td>The principals associated with the thing.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>member: PrincipalArn</th>
</tr>
</thead>
<tbody>
<tr>
<td>java class: java.util.List</td>
</tr>
</tbody>
</table>
Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

ResourceNotFoundException

The specified resource does not exist.

ListThingRegistrationTaskReports

Information about the thing registration tasks.

https

Request syntax:

GET /thing-registration-tasks/taskId/reports?reportType=reportType&maxResults=maxResults&nextToken=nextToken

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>TaskId</td>
<td>yes</td>
<td>The id of the task.</td>
</tr>
<tr>
<td>reportType</td>
<td>ReportType</td>
<td>yes</td>
<td>The type of task report.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>RegistryMaxResults</td>
<td>no</td>
<td>The maximum number of results to return per request.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json
```json
{
    "resourceLinks": [
        "string"
    ],
    "reportType": "string",
    "nextToken": "string"
}
```

### Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>resourceLinks</td>
<td>S3FileUrlList</td>
<td>no</td>
<td>Links to the task resources.</td>
</tr>
<tr>
<td>reportType</td>
<td>ReportType</td>
<td>no</td>
<td>The type of task report.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

### Errors:

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**UnauthorizedException**

You are not authorized to perform this operation.

HTTP response code: 401

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

### Synopsis:
aws iot list-thing-registration-task-reports
  --task-id <value> \
  --report-type <value> \
  [--next-token <value>] \
  [--max-results <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]

cli-input-json format:

{
  "taskId": "string",
  "reportType": "string",
  "nextToken": "string",
  "maxResults": "integer"
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>string</td>
<td>The id of the task.</td>
</tr>
<tr>
<td></td>
<td>length- max:40</td>
<td></td>
</tr>
<tr>
<td>reportType</td>
<td>string</td>
<td>The type of task report.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: ERRORS</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return per request.</td>
</tr>
<tr>
<td></td>
<td>range- max:250 min:1</td>
<td></td>
</tr>
</tbody>
</table>

Output:

{
  "resourceLinks": [ 
    "string"
  ],
  "reportType": "string",
  "nextToken": "string"
}

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>resourceLinks</td>
<td>list</td>
<td>Links to the task resources.</td>
</tr>
<tr>
<td></td>
<td>member: S3FileUrl</td>
<td></td>
</tr>
<tr>
<td>reportType</td>
<td>string</td>
<td>The type of task report.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: ERRORS</td>
</tr>
</tbody>
</table>
ListThingRegistrationTasks

List bulk thing provisioning tasks.

https

Request syntax:

GET /thing-registration-tasks?maxResults=maxResults&nextToken=nextToken&status=status

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>RegistryMaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td>status</td>
<td>Status</td>
<td>no</td>
<td>The status of the bulk thing provisioning task.</td>
</tr>
</tbody>
</table>

Response syntax:
Content-type: application/json

{
  "taskIds": [
    "string"
  ],
  "nextToken": "string"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskIds</td>
<td>TaskIdList</td>
<td>no</td>
<td>A list of bulk thing provisioning task IDs.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

aws iot list-thing-registration-tasks \
    [--next-token <value>] \
    [--max-results <value>] \
    [--status <value>] \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
**cli-input-json format:**

```json
{
   "nextToken": "string",
   "maxResults": "integer",
   "status": "string"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the bulk thing provisioning task.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: InProgress</td>
</tr>
</tbody>
</table>

**Output:**

```json
{
   "taskIds": ["string"],
   "nextToken": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskIds</td>
<td>list</td>
<td>A list of bulk thing provisioning task IDs.</td>
</tr>
<tr>
<td></td>
<td>member: TaskId</td>
<td></td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

**Errors:**

invalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

throttlingException

The rate exceeds the limit.
List Thing Types

Lists the existing thing types.

https

Request syntax:

```
GET /thing-types?maxResults=maxResults&nextToken=nextToken&thingTypeName=thingTypeName
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>RegistryMaxResults</td>
<td>no</td>
<td>The maximum number of results to return in this operation.</td>
</tr>
<tr>
<td>thingTypeName</td>
<td>ThingTypeName</td>
<td>no</td>
<td>The name of the thing type.</td>
</tr>
</tbody>
</table>

Response syntax:

```
Content-type: application/json
{
    "thingTypes": [
    {
        "thingTypeName": "string",
        "thingTypeArn": "string",
        "thingTypeProperties": {
            "thingTypeDescription": "string",
            "searchableAttributes": [
                "string"
            ],
        },
        "thingTypeMetadata": {
            "deprecated": "boolean",
            "deprecationDate": "timestamp",
            "creationDate": "timestamp"
        }
    }],
    "nextToken": "string"
}
```
Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypes</td>
<td>ThingTypeList</td>
<td>no</td>
<td>The thing types.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```bash
aws iot list-thing-types
   [--next-token <value>] \
   [--max-results <value>] \
   [--thing-type-name <value>] \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
```
"nextToken": "string",
"maxResults": "integer",
"thingTypeName": "string"
}

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return in this operation.</td>
</tr>
<tr>
<td>thingTypeName</td>
<td>string</td>
<td>The name of the thing type.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>string</td>
<td>The name of the thing type.</td>
</tr>
</tbody>
</table>

**Output:**

```
{
  "thingTypes": [
    {
      "thingTypeName": "string",
      "thingTypeArn": "string",
      "thingTypeProperties": {
        "thingTypeDescription": "string",
        "searchableAttributes": [
          "string"
        ]
      },
      "thingTypeMetadata": {
        "deprecated": "boolean",
        "deprecationDate": "timestamp",
        "creationDate": "timestamp"
      }
    },
    {
      "nextToken": "string"
    }
  ]
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypes</td>
<td>list</td>
<td>The thing types.</td>
</tr>
<tr>
<td>thingTypeName</td>
<td>string</td>
<td>The name of the thing type.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>string</td>
<td>The name of the thing type.</td>
</tr>
</tbody>
</table>

### ListThingTypes

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeArn</td>
<td>string</td>
<td>The thing type ARN.</td>
</tr>
<tr>
<td>thingTypeProperties</td>
<td>ThingTypeProperties</td>
<td>The ThingTypeProperties for the thing type.</td>
</tr>
<tr>
<td>thingTypeDescription</td>
<td>string</td>
<td>The description of the thing type.</td>
</tr>
<tr>
<td>length- max:2028</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pattern: [\p{Graph}]*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>searchableAttributes</td>
<td>list</td>
<td>A list of searchable thing attribute names.</td>
</tr>
<tr>
<td>member: AttributeName</td>
<td></td>
<td></td>
</tr>
<tr>
<td>java class: java.util.List</td>
<td></td>
<td></td>
</tr>
<tr>
<td>thingTypeMetadata</td>
<td>ThingTypeMetadata</td>
<td>The ThingTypeMetadata contains additional information about the thing type including: creation date and time, a value indicating whether the thing type is deprecated, and a date and time when it was deprecated.</td>
</tr>
<tr>
<td>deprecated</td>
<td>boolean</td>
<td>Whether the thing type is deprecated. If true, no new things could be associated with this type.</td>
</tr>
<tr>
<td>deprecationDate</td>
<td>timestamp</td>
<td>The date and time when the thing type was deprecated.</td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The date and time when the thing type was created.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

**ThrottlingException**

The rate exceeds the limit.

**UnauthorizedException**

You are not authorized to perform this operation.

**ServiceUnavailableException**

The service is temporarily unavailable.
ListThings

Lists your things. Use the attributeName and attributeValue parameters to filter your things. For example, calling ListThings with attributeName=Color and attributeValue=Red retrieves all things in the registry that contain an attribute Color with the value Red.

Request syntax:

GET /things?
maxResults=maxResults&nextToken=nextToken&attributeName=attributeName&attributeValue=attributeValue&thingTypeName=thingTypeName

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>RegistryMaxResults</td>
<td>no</td>
<td>The maximum number of results to return in this operation.</td>
</tr>
<tr>
<td>attributeName</td>
<td>AttributeName</td>
<td>no</td>
<td>The attribute name used to search for things.</td>
</tr>
<tr>
<td>attributeValue</td>
<td>AttributeValue</td>
<td>no</td>
<td>The attribute value used to search for things.</td>
</tr>
<tr>
<td>thingTypeName</td>
<td>ThingTypeName</td>
<td>no</td>
<td>The name of the thing type used to search for things.</td>
</tr>
</tbody>
</table>

Response syntax:

```
Content-type: application/json

{
  "things": [
    {
      "thingName": "string",
      "thingTypeName": "string",
      "thingArn": "string",
      "attributes": {
        "string": "string"
      },
      "version": "long"
    }
  ]
}
```
Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>things</td>
<td>ThingAttributeList</td>
<td>no</td>
<td>The things.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```bash
aws iot list-things
    [--next-token <value>]
    [--max-results <value>]
    [--attribute-name <value>]
    [--attribute-value <value>]
```
[--thing-type-name <value>]  \
[--cli-input-json <value>]  \
[--generate-cli-skeleton]

**cli-input-json format:**

```json
{
   "nextToken": "string",
   "maxResults": "integer",
   "attributeName": "string",
   "attributeValue": "string",
   "thingTypeName": "string"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>range- max:250 min:1 The maximum number of results to return in this operation.</td>
</tr>
<tr>
<td>attributeName</td>
<td>string</td>
<td>length- max:128 pattern: [a-zA-Z0-9_.@/:#-]+ The attribute name used to search for things.</td>
</tr>
<tr>
<td>attributeValue</td>
<td>string</td>
<td>length- max:800 pattern: [a-zA-Z0-9_.@/:#-]* The attribute value used to search for things.</td>
</tr>
<tr>
<td>thingTypeName</td>
<td>string</td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9_:-]+ The name of the thing type used to search for things.</td>
</tr>
</tbody>
</table>

**Output:**

```json
{
   "things": [    
      {
         "thingName": "string",
         "thingTypeName": "string",
         "thingArn": "string",
         "attributes": {
            "string": "string"
         },
         "version": "long"
      }
   ],
   "nextToken": "string"
}
```
**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>things</td>
<td>list</td>
<td>The things.</td>
</tr>
<tr>
<td></td>
<td>member: ThingAttribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9;_:-]+</td>
<td></td>
</tr>
<tr>
<td>thingTypeName</td>
<td>string</td>
<td>The name of the thing type, if the thing has been associated with a type.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9;_:-]+</td>
<td></td>
</tr>
<tr>
<td>thingArn</td>
<td>string</td>
<td>The thing ARN.</td>
</tr>
<tr>
<td>attributes</td>
<td>map</td>
<td>A list of thing attributes which are name-value pairs.</td>
</tr>
<tr>
<td>version</td>
<td>long</td>
<td>The version of the thing record in the registry.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

**ThrottlingException**

The rate exceeds the limit.

**UnauthorizedException**

You are not authorized to perform this operation.

**ServiceUnavailableException**

The service is temporarily unavailable.

**InternalFailureException**

An unexpected error has occurred.

---

**ListThingsInThingGroup**

Lists the things in the specified group.
Request syntax:

GET /thing-groups/thingGroupName/things?
recursive=recursive&maxResults=maxResults&nextToken=nextToken

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>ThingGroupName</td>
<td>yes</td>
<td>The thing group name.</td>
</tr>
<tr>
<td>recursive</td>
<td>Recursive</td>
<td>no</td>
<td>When true, list things in this thing group and in all child groups as well.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>RegistryMaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```json
{
  "things": [
    "string"
  ],
  "nextToken": "string"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>things</td>
<td>ThingNameList</td>
<td>no</td>
<td>The things in the specified thing group.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400
InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

cli

Synopsis:

```
aws iot list-things-in-thing-group
--thing-group-name <value> \
[--recursive | --no-recursive] \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "thingGroupName": "string",
  "recursive": "boolean",
  "nextToken": "string",
  "maxResults": "integer"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>string</td>
<td>The thing group name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9_:-_]+</td>
<td></td>
</tr>
<tr>
<td>recursive</td>
<td>boolean</td>
<td>When true, list things in this thing group and in all child groups as well.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token to retrieve the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td></td>
<td>range- max:250 min:1</td>
<td></td>
</tr>
</tbody>
</table>
Output:

```
{
  "things": [
    "string"
  ],
  "nextToken": "string"
}
```

### cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>things</td>
<td>list</td>
<td>The things in the specified thing group.</td>
</tr>
<tr>
<td></td>
<td>member: ThingName</td>
<td></td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

### Errors:

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **InternalFailureException**
  
  An unexpected error has occurred.

- **ResourceNotFoundException**
  
  The specified resource does not exist.

- **ThrottlingException**
  
  The rate exceeds the limit.

## ListTopicRules

Lists the rules for the specific topic.

**https**

### Request syntax:

```
GET /rules?topic=topic&maxResults=maxResults&nextToken=nextToken&ruleDisabled=ruleDisabled
```

### URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>topic</td>
<td>Topic</td>
<td>no</td>
<td>The topic.</td>
</tr>
<tr>
<td>maxResults</td>
<td>GEMaxResults</td>
<td>no</td>
<td>The maximum number of results to return.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Req?</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------</td>
<td>------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token used to retrieve the next value.</td>
</tr>
<tr>
<td>ruleDisabled</td>
<td>IsDisabled</td>
<td>no</td>
<td>Specifies whether the rule is disabled.</td>
</tr>
</tbody>
</table>

**Response syntax:**

```json
Content-type: application/json
{
  "rules": [
    { "ruleArn": "string", "ruleName": "string", "topicPattern": "string", "createdAt": "timestamp", "ruleDisabled": "boolean" }
  ],
  "nextToken": "string"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rules</td>
<td>TopicRuleList</td>
<td>no</td>
<td>The rules.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token used to retrieve the next value.</td>
</tr>
</tbody>
</table>

**Errors:**

**InternalException**

An unexpected error has occurred.

HTTP response code: 500

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ServiceUnavailableException**

The service is temporarily unavailable.

HTTP response code: 503

**cli**

**Synopsis:**
aws iot list-topic-rules
   [--topic <value>] \
   [--max-results <value>] \
   [--next-token <value>] \
   [--rule-disabled | --no-rule-disabled] \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]

cli-input-json format:

```json
{
    "topic": "string",
    "maxResults": "integer",
    "nextToken": "string",
    "ruleDisabled": "boolean"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>topic</td>
<td>string</td>
<td>The topic.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return.</td>
</tr>
<tr>
<td></td>
<td>range: max:10000 min:1</td>
<td></td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>A token used to retrieve the next value.</td>
</tr>
<tr>
<td>ruleDisabled</td>
<td>boolean</td>
<td>Specifies whether the rule is disabled.</td>
</tr>
</tbody>
</table>

Output:

```json
{
    "rules": [
        {
            "ruleArn": "string",
            "ruleName": "string",
            "topicPattern": "string",
            "createdAt": "timestamp",
            "ruleDisabled": "boolean"
        },
        {
            "ruleArn": "string",
            "ruleName": "string",
            "topicPattern": "string",
            "createdAt": "timestamp",
            "ruleDisabled": "boolean"
        }
    ],
    "nextToken": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rules</td>
<td>list</td>
<td>The rules.</td>
</tr>
<tr>
<td></td>
<td>member: TopicRuleListItem</td>
<td></td>
</tr>
<tr>
<td>ruleArn</td>
<td>string</td>
<td>The rule ARN.</td>
</tr>
<tr>
<td>ruleName</td>
<td>string</td>
<td>The name of the rule.</td>
</tr>
</tbody>
</table>
ListV2LoggingLevels

Lists logging levels.

https

Request syntax:

GET /v2LoggingLevel?maxResults=maxResults&nextToken=nextToken&targetType=targetType

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targetType</td>
<td>LogTargetType</td>
<td>no</td>
<td>The type of resource for which you are configuring logging. Must be THING_Group.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>
### ListV2LoggingLevels

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxResults</td>
<td>SkyfallMaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>

#### Response syntax:

```json
Content-type: application/json

{
  "logTargetConfigurations": [
    {
      "logTarget": {
        "targetType": "string",
        "targetName": "string"
      },
      "logLevel": "string"
    },
    "nextToken": "string"
  ]
}
```

#### Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logTargetConfigurations</td>
<td>LogTargetConfigurations</td>
<td>no</td>
<td>The logging configuration for a target.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

#### Errors:

**InternalException**

An unexpected error has occurred.

HTTP response code: 500

**NotConfiguredException**

The resource is not configured.

HTTP response code: 404

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400
ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

cli

Synopsis:

```cli
aws iot list-v2-logging-levels \
   [--target-type <value>] \
   [--next-token <value>] \
   [--max-results <value>] \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
   "targetType": "string",
   "nextToken": "string",
   "maxResults": "integer"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targetType</td>
<td>string</td>
<td>The type of resource for which you are configuring logging. Must be THING_Group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: DEFAULT</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>range- max:250 min:1</td>
</tr>
</tbody>
</table>

Output:

```json
{
   "logTargetConfigurations": [
      {
         "logTarget": {
            "targetType": "string",
            "targetName": "string"
         },
         "logLevel": "string"
      },
      {
         "nextToken": "string"
      }
   ]
}
```
cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logTargetConfigurations</td>
<td>list member: LogTargetConfiguration</td>
<td>The logging configuration for a target.</td>
</tr>
<tr>
<td>logTarget</td>
<td>LogTarget</td>
<td>A log target</td>
</tr>
<tr>
<td>targetType</td>
<td>string</td>
<td>The target type. Enum: DEFAULT</td>
</tr>
<tr>
<td>targetName</td>
<td>string</td>
<td>The target name.</td>
</tr>
<tr>
<td>logLevel</td>
<td>string</td>
<td>The logging level. Enum: DEBUG</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

- **InternalException**
  
  An unexpected error has occurred.

- **NotConfiguredException**
  
  The resource is not configured.

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ServiceUnavailableException**
  
  The service is temporarily unavailable.

**ListViolationEvents**

Lists the Device Defender security profile violations discovered during the given time period. You can use filters to limit the results to those alerts issued for a particular security profile, behavior or thing (device).

**https**

**Request syntax:**

```plaintext
GET /violation-events?
maxResults=maxResults&nextToken=nextToken&startTime=startTime&endTime=endTime&thingName=thingName&securityProfileName=securityProfileName
```
URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startTime</td>
<td>Timestamp</td>
<td>yes</td>
<td>The start time for the alerts to be listed.</td>
</tr>
<tr>
<td>endTime</td>
<td>Timestamp</td>
<td>yes</td>
<td>The end time for the alerts to be listed.</td>
</tr>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>no</td>
<td>A filter to limit results to those alerts caused by the specified thing.</td>
</tr>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>no</td>
<td>A filter to limit results to those alerts generated by the specified security profile.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>MaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
</tbody>
</table>

Response syntax:

```json
Content-type: application/json

{
  "violationEvents": [
    {
      "violationId": "string",
      "thingName": "string",
      "securityProfileName": "string",
      "behavior": {
        "name": "string",
        "metric": "string",
        "criteria": {
          "comparisonOperator": "string",
          "value": {
            "count": "long",
            "cidrs": [
              "string"
            ],
            "ports": [
              "integer"
            ]
          },
          "durationSeconds": "integer"
        }
      },
      "metricValue": {
        "count": "long",
        "cidrs": [
          "string"
        ],
        "ports": [
          "integer"
        ]
      }
    }
  ]
}```
ListViolationEvents

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>violationEvents</td>
<td>ViolationEvents</td>
<td>no</td>
<td>The security profile violation alerts issued for this account during the given time frame, potentially filtered by security profile, behavior violated, or thing (device) violating.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException
The rate exceeds the limit.

HTTP response code: 429

InternalFailureException
An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot list-violation-events \  
    --start-time <value> \  
    --end-time <value> \  
    [--thing-name <value>] \  
    [--security-profile-name <value>] \  
    [--next-token <value>] \  
```
ListViolationEvents

[--max-results <value>] \ 
[--cli-input-json <value>] \ 
[--generate-cli-skeleton]

cli-input-json format:

{
  "startTime": "timestamp",
  "endTime": "timestamp",
  "thingName": "string",
  "securityProfileName": "string",
  "nextToken": "string",
  "maxResults": "integer"
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startTime</td>
<td>timestamp</td>
<td>The start time for the alerts to be listed.</td>
</tr>
<tr>
<td>endTime</td>
<td>timestamp</td>
<td>The end time for the alerts to be listed.</td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>A filter to limit results to those alerts caused by the specified thing.</td>
</tr>
<tr>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>A filter to limit results to those alerts generated by the specified security profile.</td>
</tr>
<tr>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token for the next set of results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td>range- max:250 min:1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Output:

{
  "violationEvents": [ 
    
    "violationId": "string",
    "thingName": "string",
    "securityProfileName": "string",
    "behavior": { 
      "name": "string",
      "metric": "string",
      "criteria": { 
        "comparisonOperator": "string",
        "value": { 
          "count": "long",
          "cidrs": [ 
            "cidr1",
            "cidr2",
            "cidr3"
          ]
        }
      }
    }
  ]
}
"string"
],
"ports": [
"integer"
],
"durationSeconds": "integer"
},
"metricValue": {
"count": "long",
"cidrs": [
"string"
],
"ports": [
"integer"
],
"violationEventType": "string",
"violationEventTime": "timestamp"
},
"nextToken": "string"
}
]

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>violationEvents</td>
<td>list</td>
<td>The security profile violation alerts issued for this account during the given time frame, potentially filtered by security profile, behavior violated, or thing (device) violating.</td>
</tr>
<tr>
<td>violationId</td>
<td>string</td>
<td>The ID of the violation event.</td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing responsible for the violation event.</td>
</tr>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name of the security profile whose behavior was violated.</td>
</tr>
<tr>
<td>behavior</td>
<td>Behavior</td>
<td>The behavior which was violated.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the behavior.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>metric</td>
<td>string</td>
<td>What is measured by the behavior.</td>
</tr>
<tr>
<td>criteria</td>
<td>BehaviorCriteria</td>
<td>The criteria that determine if a device is behaving normally in regard to the metric.</td>
</tr>
<tr>
<td>comparisonOperator</td>
<td>string</td>
<td>The operator that relates the thing measured (metric) to the criteria (value).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: less-than</td>
</tr>
<tr>
<td>value</td>
<td>MetricValue</td>
<td>The value to be compared with the metric.</td>
</tr>
<tr>
<td>count</td>
<td>long</td>
<td>If the comparisonOperator calls for a numeric value, use this to specify that numeric value to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>range- min:0</td>
<td></td>
</tr>
<tr>
<td>cidrs</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of CIDRs, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>member: Cidr</td>
<td></td>
</tr>
<tr>
<td>ports</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of ports, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>member: Port</td>
<td></td>
</tr>
<tr>
<td>durationSeconds</td>
<td>integer</td>
<td>Use this to specify the period of time over which the behavior is evaluated, for those criteria which have a time dimension (for example, NUM_MESSAGES_SENT).</td>
</tr>
<tr>
<td>metricValue</td>
<td>MetricValue</td>
<td>The value of the metric (the measurement).</td>
</tr>
<tr>
<td>count</td>
<td>long</td>
<td>If the comparisonOperator calls for a numeric value, use this to specify that numeric value to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>range- min:0</td>
<td></td>
</tr>
<tr>
<td>cidrs</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of CIDRs, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>member: Cidr</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ports</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of ports, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>violationEventType</td>
<td>string</td>
<td>The type of violation event. enum: in-alarm</td>
</tr>
<tr>
<td>violationEventTime</td>
<td>timestamp</td>
<td>The time the violation event occurred.</td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>A token that can be used to retrieve the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

Publish

Publishes state information.

For more information, see HTTP Protocol in the AWS IoT Developer Guide.

https

Request syntax:

```plaintext
POST /topics/topic?qos=qos
Content-type: application/json

{
  "payload": "blob"
}
```
### URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>topic</td>
<td>Topic</td>
<td>no</td>
<td>The name of the MQTT topic.</td>
</tr>
<tr>
<td>qos</td>
<td>Qos</td>
<td>no</td>
<td>The Quality of Service (QoS) level.</td>
</tr>
</tbody>
</table>

### Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>payload</td>
<td>Payload</td>
<td>no</td>
<td>The state information, in JSON format.</td>
</tr>
</tbody>
</table>

### Errors:

- **InternalFailureException**
  
  An unexpected error has occurred.
  
  HTTP response code: 500

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  
  HTTP response code: 400

- **UnauthorizedException**
  
  You are not authorized to perform this operation.
  
  HTTP response code: 401

- **MethodNotAllowedException**
  
  The specified combination of HTTP verb and URI is not supported.
  
  HTTP response code: 405

### cli

#### Synopsis:

```bash
```

#### cli-input-json format:

```json
{
```
"topic": "string",
"qos": "integer",
"payload": "blob"
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>topic</td>
<td>string</td>
<td>The name of the MQTT topic.</td>
</tr>
<tr>
<td>qos</td>
<td>integer</td>
<td>The Quality of Service (QoS) level.</td>
</tr>
<tr>
<td>payload</td>
<td>blob</td>
<td>The state information, in JSON format.</td>
</tr>
</tbody>
</table>

Output:
None

Errors:

InternalFailureException
An unexpected error has occurred.

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

UnauthorizedException
You are not authorized to perform this operation.

MethodNotAllowedException
The specified combination of HTTP verb and URI is not supported.

RegisterCACertificate

Registers a CA certificate with AWS IoT. This CA certificate can then be used to sign device certificates, which can be then registered with AWS IoT. You can register up to 10 CA certificates per AWS account that have the same subject field. This enables you to have up to 10 certificate authorities sign your device certificates. If you have more than one CA certificate registered, make sure you pass the CA certificate when you register your device certificates with the RegisterCertificate API.

https

Request syntax:

```
POST /cacertificate?setAsActive=setAsActive&allowAutoRegistration=allowAutoRegistration
Content-type: application/json
```
RegisterCA Certificate

```
{
    "caCertificate": "string",
    "verificationCertificate": "string",
    "registrationConfig": {
        "templateBody": "string",
        "roleArn": "string"
    }
}
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>setAsActive</td>
<td>SetAsActive</td>
<td>no</td>
<td>A boolean value that specifies if the CA certificate is set to active.</td>
</tr>
<tr>
<td>allowAutoRegistration</td>
<td>AllowAutoRegistration</td>
<td>no</td>
<td>Allows this CA certificate to be used for auto registration of device certificates.</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>registrationConfig</td>
<td>RegistrationConfig</td>
<td>no</td>
<td>Information about the registration configuration.</td>
</tr>
</tbody>
</table>

**Response syntax:**

```
Content-type: application/json

{
    "certificateArn": "string",
    "certificateId": "string"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateArn</td>
<td>CertificateArn</td>
<td>no</td>
<td>The CA certificate ARN.</td>
</tr>
<tr>
<td>certificateId</td>
<td>CertificateId</td>
<td>no</td>
<td>The CA certificate identifier.</td>
</tr>
</tbody>
</table>

**Errors:**
ResourceAlreadyExistsException

The resource already exists.

HTTP response code: 409

RegistrationCodeValidationException

The registration code is invalid.

HTTP response code: 400

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

CertificateValidationException

The certificate is invalid.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

LimitExceededException

A limit has been exceeded.

HTTP response code: 410

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

aws iot register-ca-certificate \
    --ca-certificate <value> \
    --verification-certificate <value> \
    [--set-as-active | --no-set-as-active] \

RegisterCACertificate

[--allow-auto-registration | --no-allow-auto-registration] \n[--registration-config <value>] \n[--cli-input-json <value>] \n[--generate-cli-skeleton]

cli-input-json format:

{
  "caCertificate": "string",
  "verificationCertificate": "string",
  "setAsActive": "boolean",
  "allowAutoRegistration": "boolean",
  "registrationConfig": {
    "templateBody": "string",
    "roleArn": "string"
  }
}

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>caCertificate</td>
<td>string</td>
<td>The CA certificate.</td>
</tr>
<tr>
<td></td>
<td>length- max:65536 min:1</td>
<td></td>
</tr>
<tr>
<td>verificationCertificate</td>
<td>string</td>
<td>The private key verification certificate.</td>
</tr>
<tr>
<td></td>
<td>length- max:65536 min:1</td>
<td></td>
</tr>
<tr>
<td>setAsActive</td>
<td>boolean</td>
<td>A boolean value that specifies if the CA certificate is set to active.</td>
</tr>
<tr>
<td>allowAutoRegistration</td>
<td>boolean</td>
<td>Allows this CA certificate to be used for auto registration of device certificates.</td>
</tr>
<tr>
<td>registrationConfig</td>
<td>RegistrationConfig</td>
<td>Information about the registration configuration.</td>
</tr>
<tr>
<td>templateBody</td>
<td>string</td>
<td>The template body.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role.</td>
</tr>
<tr>
<td></td>
<td>length- max:2048 min:20</td>
<td></td>
</tr>
</tbody>
</table>

Output:

{
  "certificateArn": "string",
  "certificateId": "string"
}

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateArn</td>
<td>string</td>
<td>The CA certificate ARN.</td>
</tr>
</tbody>
</table>
RegisterCertificate

Registers a device certificate with AWS IoT. If you have more than one CA certificate that has the same subject field, you must specify the CA certificate that was used to sign the device certificate being registered.

**https**

**Request syntax:**

```plaintext
POST /certificate/register?setAsActive=setAsActive
Content-type: application/json
{
```
"certificatePem": "string",
"caCertificatePem": "string",
"status": "string"
}

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>setAsActive</td>
<td>SetAsActiveFlag</td>
<td>no</td>
<td>A boolean value that specifies if the CA certificate is set to active.</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificatePem</td>
<td>CertificatePem</td>
<td>yes</td>
<td>The certificate data, in PEM format.</td>
</tr>
<tr>
<td>caCertificatePem</td>
<td>CertificatePem</td>
<td>no</td>
<td>The CA certificate used to sign the device certificate being registered.</td>
</tr>
<tr>
<td>status</td>
<td>CertificateStatus</td>
<td>no</td>
<td>The status of the register certificate request.</td>
</tr>
</tbody>
</table>

**Response syntax:**

```
Content-type: application/json

{
  "certificateArn": "string",
  "certificateId": "string"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateArn</td>
<td>CertificateArn</td>
<td>no</td>
<td>The certificate ARN.</td>
</tr>
<tr>
<td>certificateId</td>
<td>CertificateId</td>
<td>no</td>
<td>The certificate identifier.</td>
</tr>
</tbody>
</table>

**Errors:**

`ResourceAlreadyExistsException`

The resource already exists.

HTTP response code: 409
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

CertificateValidationException

The certificate is invalid.

HTTP response code: 400

CertificateStateException

The certificate operation is not allowed.

HTTP response code: 406

CertificateConflictException

Unable to verify the CA certificate used to sign the device certificate you are attempting to register. This happens when you have registered more than one CA certificate that has the same subject field and public key.

HTTP response code: 409

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot register-certificate \   
   --certificate-pem <value> \   
   [--ca-certificate-pem <value>] \   
   [--set-as-active | --no-set-as-active] \   
   [--status <value>] \   
   [--cli-input-json <value>] \   
   [--generate-cli-skeleton]
```
cli-input-json format:

```json
{
   "certificatePem": "string",
   "caCertificatePem": "string",
   "status": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificatePem</td>
<td>string</td>
<td>The certificate data, in PEM format.</td>
</tr>
<tr>
<td></td>
<td>length- max:65536 min:1</td>
<td></td>
</tr>
<tr>
<td>caCertificatePem</td>
<td>string</td>
<td>The CA certificate used to sign the device certificate being registered.</td>
</tr>
<tr>
<td></td>
<td>length- max:65536 min:1</td>
<td></td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the register certificate request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: ACTIVE</td>
</tr>
</tbody>
</table>

Output:

```json
{
   "certificateArn": "string",
   "certificateId": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateArn</td>
<td>string</td>
<td>The certificate ARN.</td>
</tr>
<tr>
<td>certificateId</td>
<td>string</td>
<td>The certificate identifier.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: (0x)?[a-fA-F0-9]+</td>
<td></td>
</tr>
</tbody>
</table>

Errors:

ResourceAlreadyExistsException

The resource already exists.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
CertificateValidationException

The certificate is invalid.

CertificateStateException

The certificate operation is not allowed.

CertificateConflictException

Unable to verify the CA certificate used to sign the device certificate you are attempting to register. This happens when you have registered more than one CA certificate that has the same subject field and public key.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalServerError

An unexpected error has occurred.

---

**RegisterThing**

Provisions a thing.

https

**Request syntax:**

```
POST /things
Content-type: application/json

{
  "templateBody": "string",
  "parameters": {
    "string": "string"
  }
}
```

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>templateBody</td>
<td>TemplateBody</td>
<td>yes</td>
<td>The provisioning template. See Programmatic Provisioning for more information.</td>
</tr>
<tr>
<td>parameters</td>
<td>Parameters</td>
<td>no</td>
<td>The parameters for provisioning a thing. See Programmatic</td>
</tr>
</tbody>
</table>
RegisterThing

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Provisioning for more information.</td>
</tr>
</tbody>
</table>

Response syntax:

```json
Content-type: application/json

{
  "certificatePem": "string",
  "resourceArns": {
    "string": "string"
  }
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificatePem</td>
<td>CertificatePem</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>resourceArns</td>
<td>ResourceArns</td>
<td>no</td>
<td>ARNs for the generated resources.</td>
</tr>
</tbody>
</table>

Errors:

InternalFailureException
  - An unexpected error has occurred.
  - HTTP response code: 500

ServiceUnavailableException
  - The service is temporarily unavailable.
  - HTTP response code: 503

InvalidRequestException
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  - HTTP response code: 400

UnauthorizedException
  - You are not authorized to perform this operation.
  - HTTP response code: 401

ThrottlingException
  - The rate exceeds the limit.
  - HTTP response code: 429

ConflictingResourceUpdateException
  - A conflicting resource update exception. This exception is thrown when two pending updates cause a conflict.
HTTP response code: 409
ResourceRegistrationFailureException

The resource registration failed.

HTTP response code: 400

cli

Synopsis:

```
aws iot register-thing \
   --template-body <value> \ 
   [--parameters <value>] \ 
   [--cli-input-json <value>] \ 
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "templateBody": "string",
   "parameters": {
       "string": "string"
   }
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>templateBody</td>
<td>string</td>
<td>The provisioning template. See Programmatic Provisioning for more information.</td>
</tr>
<tr>
<td>parameters</td>
<td>map</td>
<td>The parameters for provisioning a thing. See Programmatic Provisioning for more information.</td>
</tr>
</tbody>
</table>

Output:

```
{
   "certificatePem": "string",
   "resourceArns": {
       "string": "string"
   }
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificatePem</td>
<td>string</td>
<td>length: max:65536 min:1</td>
</tr>
</tbody>
</table>
RejectCertificateTransfer

Rejects a pending certificate transfer. After AWS IoT rejects a certificate transfer, the certificate status changes from **PENDING_TRANSFER** to **INACTIVE**.

To check for pending certificate transfers, call ListCertificates to enumerate your certificates.

This operation can only be called by the transfer destination. After it is called, the certificate will be returned to the source's account in the INACTIVE state.

### Request syntax:

```
PATCH /reject-certificate-transfer/certificateId
Content-type: application/json

{
  "rejectReason": "string"
}
```
URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>CertificateId</td>
<td>yes</td>
<td>The ID of the certificate. (The last part of the certificate ARN contains the certificate ID.)</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rejectReason</td>
<td>Message</td>
<td>no</td>
<td>The reason the certificate transfer was rejected.</td>
</tr>
</tbody>
</table>

Errors:

- **ResourceNotFoundException**
  - The specified resource does not exist.
  - HTTP response code: 404

- **TransferAlreadyCompletedException**
  - You can't revert the certificate transfer because the transfer is already complete.
  - HTTP response code: 410

- **InvalidRequestException**
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  - HTTP response code: 400

- **ThrottlingException**
  - The rate exceeds the limit.
  - HTTP response code: 429

- **UnauthorizedException**
  - You are not authorized to perform this operation.
  - HTTP response code: 401

- **ServiceUnavailableException**
  - The service is temporarily unavailable.
  - HTTP response code: 503

- **InternalFailureException**
  - An unexpected error has occurred.
  - HTTP response code: 500
cli

Synopsis:

```
aws iot reject-certificate-transfer \\
    --certificate-id <value> \\
    [--reject-reason <value>] \\
    [--cli-input-json <value>] \\
    [--generate-cli-skeleton]
```

cli-input-json format:

```
{
    "certificateId": "string",
    "rejectReason": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>string</td>
<td>length: max:64 min:64 pattern: (0x)?[a-fA-F0-9]+</td>
</tr>
<tr>
<td>rejectReason</td>
<td>string</td>
<td>length: max:128</td>
</tr>
</tbody>
</table>

Output:

None

Errors:

ResourceNotFoundException

The specified resource does not exist.

TransferAlreadyCompletedException

You can't revert the certificate transfer because the transfer is already complete.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.
InternalFailureException

An unexpected error has occurred.

RemoveThingFromThingGroup

Remove the specified thing from the specified group.

https

Request syntax:

```
PUT /thing-groups/removeThingFromThingGroup
Content-type: application/json

{
  "thingGroupName": "string",
  "thingGroupArn": "string",
  "thingName": "string",
  "thingArn": "string"
}
```

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>ThingGroupName</td>
<td>no</td>
<td>The group name.</td>
</tr>
<tr>
<td>thingGroupArn</td>
<td>ThingGroupArn</td>
<td>no</td>
<td>The group ARN.</td>
</tr>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>no</td>
<td>The name of the thing to remove from the group.</td>
</tr>
<tr>
<td>thingArn</td>
<td>ThingArn</td>
<td>no</td>
<td>The ARN of the thing to remove from the group.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500
ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

cli

Synopsis:

```
aws iot remove-thing-from-thing-group \
    [--thing-group-name <value>] \
    [--thing-group-arn <value>] \
    [--thing-name <value>] \
    [--thing-arn <value>] \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

cli-input-json format:

```
{
    "thingGroupName": "string",
    "thingGroupArn": "string",
    "thingName": "string",
    "thingArn": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>string</td>
<td>The group name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:-_]+</td>
<td></td>
</tr>
<tr>
<td>thingGroupArn</td>
<td>string</td>
<td>The group ARN.</td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing to remove from the group.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:-_]+</td>
<td></td>
</tr>
<tr>
<td>thingArn</td>
<td>string</td>
<td>The ARN of the thing to remove from the group.</td>
</tr>
</tbody>
</table>

Output:

None

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.

ResourceNotFoundException

The specified resource does not exist.

ReplaceTopicRule

Replaces the rule. You must specify all parameters for the new rule. Creating rules is an administrator-level action. Any user who has permission to create rules will be able to access data processed by the rule.

https

Request syntax:

PATCH /rules/ruleName
Content-type: application/json

{  "topicRulePayload": {  "sql": "string",  "description": "string",  "actions": [  {  "dynamoDB": {  "tableName": "string",  "roleArn": "string",  "operation": "string",  "hashKeyField": "string",  "hashKeyValue": "string",  "hashKeyType": "string",  "rangeKeyField": "string",  "rangeKeyValue": "string",  "rangeKeyType": "string",  "payloadField": "string"  },  "dynamoDBv2": {  "roleArn": "string",  "putItem": {  "tableName": "string"  }  },  "lambda": {  "functionArn": "string"  },  "sns": {  "targetArn": "string",  "roleArn": "string",  "messageFormat": "string"  },  "sqs": {  "roleArn": "string",  "queueUrl": "string",  "useBase64": "boolean"  }  ]  }  }
"kinesis": {
  "roleArn": "string",
  "streamName": "string",
  "partitionKey": "string"
},
"republish": {
  "roleArn": "string",
  "topic": "string"
},
"s3": {
  "roleArn": "string",
  "bucketName": "string",
  "key": "string",
  "cannedAcl": "string"
},
"firehose": {
  "roleArn": "string",
  "deliveryStreamName": "string",
  "separator": "string"
},
"cloudwatchMetric": {
  "roleArn": "string",
  "metricNamespace": "string",
  "metricName": "string",
  "metricValue": "string",
  "metricUnit": "string",
  "metricTimestamp": "string"
},
"cloudwatchAlarm": {
  "roleArn": "string",
  "alarmName": "string",
  "stateReason": "string",
  "stateValue": "string"
},
"elasticsearch": {
  "roleArn": "string",
  "endpoint": "string",
  "index": "string",
  "type": "string",
  "id": "string"
},
"salesforce": {
  "token": "string",
  "url": "string"
},
"iotAnalytics": {
  "channelArn": "string",
  "channelName": "string",
  "roleArn": "string"
},
"stepFunctions": {
  "executionNamePrefix": "string",
  "stateMachineName": "string",
  "roleArn": "string"
}
],
"ruleDisabled": "boolean",
"awsIotSqlVersion": "string",
"errorAction": {
  "dynamoDB": {
    "tableName": "string",
    "roleArn": "string",
    "operation": "string",
    "hashKeyField": "string",
    "hashKeyValue": "string"
  }
}
"hashKeyType": "string",
"rangeKeyField": "string",
"rangeKeyValue": "string",
"rangeKeyType": "string",
"payloadField": "string"
},
"dynamoDBv2": {
  "roleArn": "string",
  "putItem": {
    "tableName": "string"
  };
},
"lambda": {
  "functionArn": "string"
},
"sns": {
  "targetArn": "string",
  "roleArn": "string",
  "messageFormat": "string"
},
"sqs": {
  "roleArn": "string",
  "queueUrl": "string",
  "useBase64": "boolean"
},
"kinesis": {
  "roleArn": "string",
  "streamName": "string",
  "partitionKey": "string"
},
"republish": {
  "roleArn": "string",
  "topic": "string"
},
"s3": {
  "roleArn": "string",
  "bucketName": "string",
  "key": "string",
  "cannedAcl": "string"
},
"firehose": {
  "roleArn": "string",
  "deliveryStreamName": "string",
  "separator": "string"
},
"cloudwatchMetric": {
  "roleArn": "string",
  "metricNamespace": "string",
  "metricName": "string",
  "metricValue": "string",
  "metricUnit": "string",
  "metricTimestamp": "string"
},
"cloudwatchAlarm": {
  "roleArn": "string",
  "alarmName": "string",
  "stateReason": "string",
  "stateValue": "string"
},
"elasticsearch": {
  "roleArn": "string",
  "endpoint": "string",
  "index": "string",
  "type": "string",
  "id": "string"
}
"salesforce": {
    "token": "string",
    "url": "string"
},
"iotAnalytics": {
    "channelArn": "string",
    "channelName": "string",
    "roleArn": "string"
},
"stepFunctions": {
    "executionNamePrefix": "string",
    "stateMachineName": "string",
    "roleArn": "string"
}
}

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleName</td>
<td>RuleName</td>
<td>yes</td>
<td>The name of the rule.</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>topicRulePayload</td>
<td>TopicRulePayload</td>
<td>yes</td>
<td>The rule payload.</td>
</tr>
</tbody>
</table>

Errors:

SqlParseException

The Rule-SQL expression can't be parsed correctly.

HTTP response code: 400

InternalException

An unexpected error has occurred.

HTTP response code: 500

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

UnauthorizedException

You are not authorized to perform this operation.
HTTP response code: 401

cli

Synopsis:

```bash
aws iot replace-topic-rule \
   --rule-name <value> \ 
   --topic-rule-payload <value> \ 
   [--cli-input-json <value>] \ 
   [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
   "ruleName": "string",
   "topicRulePayload": {
      "sql": "string",
      "description": "string",
      "actions": [
         {
            "dynamoDB": {
               "tableName": "string",
               "roleArn": "string",
               "operation": "string",
               "hashKeyField": "string",
               "hashKeyValue": "string",
               "hashKeyType": "string",
               "rangeKeyField": "string",
               "rangeKeyValue": "string",
               "rangeKeyType": "string",
               "payloadField": "string"
            },
            "dynamoDBv2": {
               "roleArn": "string",
               "putItem": {
                  "tableName": "string"
               }
            },
            "lambda": {
               "functionArn": "string"
            },
            "sns": {
               "targetArn": "string",
               "roleArn": "string",
               "messageFormat": "string"
            },
            "sqs": {
               "roleArn": "string",
               "queueUrl": "string",
               "useBase64": "boolean"
            },
            "kinesis": {
               "roleArn": "string",
               "streamName": "string",
               "partitionKey": "string"
            },
            "republish": {
               "roleArn": "string",
               "topic": "string"
            }
         }
      ]
   }
}
```
"roleArn": "string",
"bucketName": "string",
"key": "string",
"cannedAcl": "string"
},
"firehose": {
"roleArn": "string",
"deliveryStreamName": "string",
"separator": "string"
},
"cloudwatchMetric": {
"roleArn": "string",
"metricNamespace": "string",
"metricName": "string",
"metricValue": "string",
"metricUnit": "string",
"metricTimestamp": "string"
},
"cloudwatchAlarm": {
"roleArn": "string",
"alarmName": "string",
"stateReason": "string",
"stateValue": "string"
},
"elasticsearch": {
"roleArn": "string",
"endpoint": "string",
"index": "string",
"type": "string",
"id": "string"
},
"salesforce": {
"token": "string",
"url": "string"
},
"iotAnalytics": {
"channelArn": "string",
"channelName": "string",
"roleArn": "string"
},
"stepFunctions": {
"executionNamePrefix": "string",
"stateMachineName": "string",
"roleArn": "string"
}
},
"ruleDisabled": "boolean",
"awsIotSqlVersion": "string",
"errorAction": {
"dynamoDB": {
"roleArn": "string",
"tableName": "string",
"operation": "string",
"hashKeyField": "string",
"hashKeyValue": "string",
"hashKeyType": "string",
"rangeKeyField": "string",
"rangeKeyValue": "string",
"rangeKeyType": "string",
"payloadField": "string"
},
"dynamoDBv2": {
"roleArn": "string",
"putItem": {
"tableName": "string"
}
"executionNamePrefix": "string",
"stateMachineName": "string",
"roleArn": "string"
}
}
}
}

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleName</td>
<td>string</td>
<td>The name of the rule.</td>
</tr>
<tr>
<td></td>
<td>length: max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: ^[a-zA-Z0-9_]+$</td>
<td></td>
</tr>
<tr>
<td>topicRulePayload</td>
<td>TopicRulePayload</td>
<td>The rule payload.</td>
</tr>
<tr>
<td>sql</td>
<td>string</td>
<td>The SQL statement used to query the topic. For more information, see AWS IoT SQL Reference in the AWS IoT Developer Guide.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>The description of the rule.</td>
</tr>
<tr>
<td>actions</td>
<td>list</td>
<td>The actions associated with the rule.</td>
</tr>
<tr>
<td></td>
<td>member: Action</td>
<td></td>
</tr>
<tr>
<td>dynamoDB</td>
<td>DynamoDBAction</td>
<td>Write to a DynamoDB table.</td>
</tr>
<tr>
<td>tableName</td>
<td>string</td>
<td>The name of the DynamoDB table.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the DynamoDB table.</td>
</tr>
<tr>
<td>operation</td>
<td>string</td>
<td>The type of operation to be performed. This follows the substitution template, so it can be $operation, but the substitution must result in one of the following: INSERT, UPDATE, or DELETE.</td>
</tr>
<tr>
<td>hashKeyField</td>
<td>string</td>
<td>The hash key name.</td>
</tr>
<tr>
<td>hashKeyValue</td>
<td>string</td>
<td>The hash key value.</td>
</tr>
<tr>
<td>hashKeyType</td>
<td>string</td>
<td>The hash key type. Valid values are &quot;STRING&quot; or &quot;NUMBER&quot;</td>
</tr>
<tr>
<td>rangeKeyField</td>
<td>string</td>
<td>The range key name.</td>
</tr>
<tr>
<td>rangeKeyValue</td>
<td>string</td>
<td>The range key value.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>rangeKeyType</td>
<td>string</td>
<td>The range key type. Valid values are &quot;STRING&quot; or &quot;NUMBER&quot;</td>
</tr>
<tr>
<td>payloadField</td>
<td>string</td>
<td>The action payload. This name can be customized.</td>
</tr>
<tr>
<td>dynamoDBv2</td>
<td>DynamoDBv2Action</td>
<td>Write to a DynamoDB table. This is a new version of the DynamoDB action. It allows you to write each attribute in an MQTT message payload into a separate DynamoDB column.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the DynamoDB table.</td>
</tr>
<tr>
<td>putItem</td>
<td>PutItemInput</td>
<td>Specifies the DynamoDB table to which the message data will be written. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{ &quot;dynamoDBv2&quot;: { &quot;roleArn&quot;: &quot;aws:iam:12341251:my-role&quot;, &quot;putItem&quot;: { &quot;tableName&quot;: &quot;my-table&quot; } } }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Each attribute in the message payload will be written to a separate column in the DynamoDB database.</td>
</tr>
<tr>
<td>tableName</td>
<td>string</td>
<td>The table where the message data will be written</td>
</tr>
<tr>
<td>lambda</td>
<td>LambdaAction</td>
<td>Invoke a Lambda function.</td>
</tr>
<tr>
<td>functionArn</td>
<td>string</td>
<td>The ARN of the Lambda function.</td>
</tr>
<tr>
<td>sns</td>
<td>SnsAction</td>
<td>Publish to an Amazon SNS topic.</td>
</tr>
<tr>
<td>targetArn</td>
<td>string</td>
<td>The ARN of the SNS topic.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>messageFormat</td>
<td>string</td>
<td>(Optional) The message format of the message to publish. Accepted values are &quot;JSON&quot; and &quot;RAW&quot;. The default value of the attribute is &quot;RAW&quot;. SNS uses this setting to determine if the payload should be parsed and relevant platform-specific bits of the payload should be extracted. To read more about SNS message formats, see <a href="http://docs.aws.amazon.com/sns/latest/dg/json-formats.html">http://docs.aws.amazon.com/sns/latest/dg/json-formats.html</a> refer to their official documentation.</td>
</tr>
<tr>
<td>sqs</td>
<td>SqsAction</td>
<td>Publish to an Amazon SQS queue.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>queueUrl</td>
<td>string</td>
<td>The URL of the Amazon SQS queue.</td>
</tr>
<tr>
<td>useBase64</td>
<td>boolean</td>
<td>Specifies whether to use Base64 encoding.</td>
</tr>
<tr>
<td>kinesis</td>
<td>KinesisAction</td>
<td>Write data to an Amazon Kinesis stream.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the Amazon Kinesis stream.</td>
</tr>
<tr>
<td>streamName</td>
<td>string</td>
<td>The name of the Amazon Kinesis stream.</td>
</tr>
<tr>
<td>partitionKey</td>
<td>string</td>
<td>The partition key.</td>
</tr>
<tr>
<td>republish</td>
<td>RepublishAction</td>
<td>Publish to another MQTT topic.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>topic</td>
<td>string</td>
<td>The name of the MQTT topic.</td>
</tr>
<tr>
<td>s3</td>
<td>S3Action</td>
<td>Write to an Amazon S3 bucket.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>bucketName</td>
<td>string</td>
<td>The Amazon S3 bucket.</td>
</tr>
<tr>
<td>key</td>
<td>string</td>
<td>The object key.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cannedAcl</td>
<td>string</td>
<td>The Amazon S3 canned ACL that controls access to the object identified by the object key. For more information, see <a href="https://docs.aws.amazon.com/AmazonS3/latest/userguide/canned-acl.html">S3 canned ACLs</a>. `&lt;enum: private</td>
</tr>
<tr>
<td>firehose</td>
<td>FirehoseAction</td>
<td>Write to an Amazon Kinesis Firehose stream.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role that grants access to the Amazon Kinesis Firehose stream.</td>
</tr>
<tr>
<td>deliveryStreamName</td>
<td>string</td>
<td>The delivery stream name.</td>
</tr>
<tr>
<td>separator</td>
<td>string</td>
<td>A character separator that will be used to separate records written to the Firehose stream. Valid values are: <code>\n</code> (newline), <code>\t</code> (tab), <code>\r\n</code> (Windows newline), <code>,</code> (comma).</td>
</tr>
<tr>
<td>cloudwatchMetric</td>
<td>CloudwatchMetricAction</td>
<td>Capture a CloudWatch metric.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role that allows access to the CloudWatch metric.</td>
</tr>
<tr>
<td>metricNamespace</td>
<td>string</td>
<td>The CloudWatch metric namespace name.</td>
</tr>
<tr>
<td>metricName</td>
<td>string</td>
<td>The CloudWatch metric name.</td>
</tr>
<tr>
<td>metricValue</td>
<td>string</td>
<td>The CloudWatch metric value.</td>
</tr>
<tr>
<td>metricUnit</td>
<td>string</td>
<td>The metric unit supported by CloudWatch.</td>
</tr>
<tr>
<td>metricTimestamp</td>
<td>string</td>
<td>An optional Unix timestamp.</td>
</tr>
<tr>
<td>cloudwatchAlarm</td>
<td>CloudwatchAlarmAction</td>
<td>Change the state of a CloudWatch alarm.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role that allows access to the CloudWatch alarm.</td>
</tr>
<tr>
<td>alarmName</td>
<td>string</td>
<td>The CloudWatch alarm name.</td>
</tr>
<tr>
<td>stateReason</td>
<td>string</td>
<td>The reason for the alarm change.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>stateValue</td>
<td>string</td>
<td>The value of the alarm state. Acceptable values are: OK, ALARM, INSUFFICIENT_DATA.</td>
</tr>
<tr>
<td>elasticsearch</td>
<td>ElasticsearchAction</td>
<td>Write data to an Amazon Elasticsearch Service domain.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role ARN that has access to Elasticsearch.</td>
</tr>
<tr>
<td>endpoint</td>
<td>string, pattern: https?://.*</td>
<td>The endpoint of your Elasticsearch domain.</td>
</tr>
<tr>
<td>index</td>
<td>string</td>
<td>The Elasticsearch index where you want to store your data.</td>
</tr>
<tr>
<td>type</td>
<td>string</td>
<td>The type of document you are storing.</td>
</tr>
<tr>
<td>id</td>
<td>string</td>
<td>The unique identifier for the document you are storing.</td>
</tr>
<tr>
<td>salesforce</td>
<td>SalesforceAction</td>
<td>Send a message to a Salesforce IoT Cloud Input Stream.</td>
</tr>
<tr>
<td>token</td>
<td>string, length- min:40</td>
<td>The token used to authenticate access to the Salesforce IoT Cloud Input Stream. The token is available from the Salesforce IoT Cloud platform after creation of the Input Stream.</td>
</tr>
<tr>
<td>url</td>
<td>string, length- max:2000 pattern: <a href="https://ingestion-%5Ba-zA-Z0-9">https://ingestion-[a-zA-Z0-9</a>][1,12],[a-zA-Z0-9]+.((sfdc-matrix.net)</td>
<td>(sfdcnow.com))/streams/w 1,20/w 1,20/event</td>
</tr>
<tr>
<td>iotAnalytics</td>
<td>IotAnalyticsAction</td>
<td>Sends message data to an AWS IoT Analytics channel.</td>
</tr>
<tr>
<td>channelArn</td>
<td>string</td>
<td>(deprecated) The ARN of the IoT Analytics channel to which message data will be sent.</td>
</tr>
<tr>
<td>channelName</td>
<td>string</td>
<td>The name of the IoT Analytics channel to which message data will be sent.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role which has a policy that grants IoT Analytics permission to send message data via IoT Analytics (iotanalytics:BatchPutMessage).</td>
</tr>
</tbody>
</table>
## ReplaceTopicRule

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stepFunctions</td>
<td>StepFunctionsAction</td>
<td>Starts execution of a Step Functions state machine.</td>
</tr>
<tr>
<td>executionNamePrefix</td>
<td>string</td>
<td>(Optional) A name will be given to the state machine execution consisting of this prefix followed by a UUID. Step Functions automatically creates a unique name for each state machine execution if one is not provided.</td>
</tr>
<tr>
<td>stateMachineName</td>
<td>string</td>
<td>The name of the Step Functions state machine whose execution will be started.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants IoT permission to start execution of a state machine (&quot;Action&quot;:&quot;states:StartExecution&quot;).</td>
</tr>
<tr>
<td>ruleDisabled</td>
<td>boolean</td>
<td>Specifies whether the rule is disabled.</td>
</tr>
<tr>
<td>awslotSqlVersion</td>
<td>string</td>
<td>The version of the SQL rules engine to use when evaluating the rule.</td>
</tr>
<tr>
<td>errorAction</td>
<td>Action</td>
<td>The action to take when an error occurs.</td>
</tr>
<tr>
<td>dynamoDB</td>
<td>DynamoDBAction</td>
<td>Write to a DynamoDB table.</td>
</tr>
<tr>
<td>tableName</td>
<td>string</td>
<td>The name of the DynamoDB table.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the DynamoDB table.</td>
</tr>
<tr>
<td>operation</td>
<td>string</td>
<td>The type of operation to be performed. This follows the substitution template, so it can be $ operation, but the substitution must result in one of the following: INSERT, UPDATE, or DELETE.</td>
</tr>
<tr>
<td>hashKeyField</td>
<td>string</td>
<td>The hash key name.</td>
</tr>
<tr>
<td>hashKeyValue</td>
<td>string</td>
<td>The hash key value.</td>
</tr>
<tr>
<td>hashKeyType</td>
<td>string</td>
<td>The hash key type. Valid values are &quot;STRING&quot; or &quot;NUMBER&quot;</td>
</tr>
<tr>
<td>rangeKeyField</td>
<td>string</td>
<td>The range key name.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>rangeKeyValue</td>
<td>string</td>
<td>The range key value.</td>
</tr>
<tr>
<td>rangeKeyType</td>
<td>string</td>
<td>The range key type. Valid values are &quot;STRING&quot; or &quot;NUMBER&quot;</td>
</tr>
<tr>
<td>payloadField</td>
<td>string</td>
<td>The action payload. This name can be customized.</td>
</tr>
<tr>
<td>dynamoDBv2</td>
<td>DynamoDBv2Action</td>
<td>Write to a DynamoDB table. This is a new version of the DynamoDB action. It allows you to write each attribute in an MQTT message payload into a separate DynamoDB column.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access to the DynamoDB table.</td>
</tr>
<tr>
<td>putItem</td>
<td>PutItemInput</td>
<td>Specifies the DynamoDB table to which the message data will be written. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{ &quot;dynamoDBv2&quot;: { &quot;roleArn&quot;: &quot;aws:iam:12341251:my-role&quot; }  &quot;putItem&quot;: { &quot;tableName&quot;: &quot;my-table&quot; } } }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Each attribute in the message payload will be written to a separate column in the DynamoDB database.</td>
</tr>
<tr>
<td>tableName</td>
<td>string</td>
<td>The table where the message data will be written</td>
</tr>
<tr>
<td>lambda</td>
<td>LambdaAction</td>
<td>Invoke a Lambda function.</td>
</tr>
<tr>
<td>functionArn</td>
<td>string</td>
<td>The ARN of the Lambda function.</td>
</tr>
<tr>
<td>sns</td>
<td>SnsAction</td>
<td>Publish to an Amazon SNS topic.</td>
</tr>
<tr>
<td>targetArn</td>
<td>string</td>
<td>The ARN of the SNS topic.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>messageFormat</td>
<td>string</td>
<td>(Optional) The message format of the message to publish. Accepted values are “JSON” and “RAW”. The default value of the attribute is “RAW”. SNS uses this setting to determine if the payload should be parsed and relevant platform-specific bits of the payload should be extracted. To read more about SNS message formats, see <a href="http://docs.aws.amazon.com/sns/latest/dg/json-formats.html">http://docs.aws.amazon.com/sns/latest/dg/json-formats.html</a> refer to their official documentation. enum: RAW</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cannedAcl</td>
<td>string</td>
<td>The Amazon S3 canned ACL that controls access to the object identified by the object key. For more information, see S3 canned ACLs.</td>
</tr>
<tr>
<td>firehose</td>
<td>FirehoseAction</td>
<td>Write to an Amazon Kinesis Firehose stream.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role that grants access to the Amazon Kinesis Firehose stream.</td>
</tr>
<tr>
<td>deliveryStreamName</td>
<td>string</td>
<td>The delivery stream name.</td>
</tr>
<tr>
<td>separator</td>
<td>string</td>
<td>A character separator that will be used to separate records written to the Firehose stream. Valid values are: 'newline', 'tab', 'Windows newline', 'comma'.</td>
</tr>
<tr>
<td>cloudwatchMetric</td>
<td>CloudwatchMetricAction</td>
<td>Capture a CloudWatch metric.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role that allows access to the CloudWatch metric.</td>
</tr>
<tr>
<td>metricNamespace</td>
<td>string</td>
<td>The CloudWatch metric namespace name.</td>
</tr>
<tr>
<td>metricName</td>
<td>string</td>
<td>The CloudWatch metric name.</td>
</tr>
<tr>
<td>metricValue</td>
<td>string</td>
<td>The CloudWatch metric value.</td>
</tr>
<tr>
<td>metricUnit</td>
<td>string</td>
<td>The metric unit supported by CloudWatch.</td>
</tr>
<tr>
<td>metricTimestamp</td>
<td>string</td>
<td>An optional Unix timestamp.</td>
</tr>
<tr>
<td>cloudwatchAlarm</td>
<td>CloudwatchAlarmAction</td>
<td>Change the state of a CloudWatch alarm.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role that allows access to the CloudWatch alarm.</td>
</tr>
<tr>
<td>alarmName</td>
<td>string</td>
<td>The CloudWatch alarm name.</td>
</tr>
<tr>
<td>stateReason</td>
<td>string</td>
<td>The reason for the alarm change.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>stateValue</td>
<td>string</td>
<td>The value of the alarm state. Acceptable values are: OK, ALARM, INSUFFICIENT_DATA.</td>
</tr>
<tr>
<td>elasticsearch</td>
<td>ElasticsearchAction</td>
<td>Write data to an Amazon Elasticsearch Service domain.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role ARN that has access to Elasticsearch.</td>
</tr>
<tr>
<td>endpoint</td>
<td>string</td>
<td>The endpoint of your Elasticsearch domain.</td>
</tr>
<tr>
<td>index</td>
<td>string</td>
<td>The Elasticsearch index where you want to store your data.</td>
</tr>
<tr>
<td>type</td>
<td>string</td>
<td>The type of document you are storing.</td>
</tr>
<tr>
<td>id</td>
<td>string</td>
<td>The unique identifier for the document you are storing.</td>
</tr>
<tr>
<td>salesforce</td>
<td>SalesforceAction</td>
<td>Send a message to a Salesforce IoT Cloud Input Stream.</td>
</tr>
<tr>
<td>token</td>
<td>string</td>
<td>The token used to authenticate access to the Salesforce IoT Cloud Input Stream. The token is available from the Salesforce IoT Cloud platform after creation of the Input Stream.</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>The URL exposed by the Salesforce IoT Cloud Input Stream. The URL is available from the Salesforce IoT Cloud platform after creation of the Input Stream.</td>
</tr>
<tr>
<td>iotAnalytics</td>
<td>IotAnalyticsAction</td>
<td>Sends message data to an AWS IoT Analytics channel.</td>
</tr>
<tr>
<td>channelArn</td>
<td>string</td>
<td>(deprecated) The ARN of the IoT Analytics channel to which message data will be sent.</td>
</tr>
<tr>
<td>channelName</td>
<td>string</td>
<td>The name of the IoT Analytics channel to which message data will be sent.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role which has a policy that grants IoT Analytics permission to send message data via IoT Analytics (iotanalytics:BatchPutMessage).</td>
</tr>
</tbody>
</table>
### Name | Type | Description
---|---|---
stepFunctions | StepFunctionsAction | Starts execution of a Step Functions state machine.
executionNamePrefix | string | (Optional) A name will be given to the state machine execution consisting of this prefix followed by a UUID. Step Functions automatically creates a unique name for each state machine execution if one is not provided.
stateMachineName | string | The name of the Step Functions state machine whose execution will be started.
roleArn | string | The ARN of the role that grants IoT permission to start execution of a state machine ("Action":"states:StartExecution").

**Output:**

None

**Errors:**

SqlParseException

The Rule-SQL expression can't be parsed correctly.

InternalException

An unexpected error has occurred.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ServiceUnavailableException

The service is temporarily unavailable.

UnauthorizedException

You are not authorized to perform this operation.

---

**SearchIndex**

The query search index.

https

**Request syntax:**

POST /indices/search
Content-type: application/json

{
   "indexName": "string",
   "queryString": "string",
   "nextToken": "string",
   "maxResults": "integer",
   "queryVersion": "string"
}

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>indexName</td>
<td>IndexName</td>
<td>no</td>
<td>The search index name.</td>
</tr>
<tr>
<td>queryString</td>
<td>QueryString</td>
<td>yes</td>
<td>The search query string.</td>
</tr>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>QueryMaxResults</td>
<td>no</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td>queryVersion</td>
<td>QueryVersion</td>
<td>no</td>
<td>The query version.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{
   "nextToken": "string",
   "things": [
      {
         "thingName": "string",
         "thingId": "string",
         "thingTypeName": "string",
         "thingGroupNames": [ "string" ],
         "attributes": {
            "string": "string"
         },
         "shadow": "string"
      }
   ]
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>NextToken</td>
<td>no</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
</tbody>
</table>
Name | Type | Req? | Description
 things | ThingDocumentList | no | The things that match the search query.

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**UnauthorizedException**

You are not authorized to perform this operation.

HTTP response code: 401

**ServiceUnavailableException**

The service is temporarily unavailable.

HTTP response code: 503

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

**ResourceNotFoundException**

The specified resource does not exist.

HTTP response code: 404

**InvalidQueryException**

The query is invalid.

HTTP response code: 400

**IndexNotReadyException**

The index is not ready.

HTTP response code: 400

**Synopsis:**

```
aws iot search-index \\
    [--index-name <value>] \\
```
aws iot developer guide
searchindex

--query-string <value> \
[--next-token <value>] \
[--max-results <value>] \
[--query-version <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]

cli-input-json format:

```json
{
   "indexName": "string",
   "queryString": "string",
   "nextToken": "string",
   "maxResults": "integer",
   "queryVersion": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>indexName</td>
<td>string</td>
<td>The search index name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>queryString</td>
<td>string</td>
<td>The search query string.</td>
</tr>
<tr>
<td></td>
<td>length- max:1000 min:1</td>
<td></td>
</tr>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
<tr>
<td>maxResults</td>
<td>integer range- max:500 min:1</td>
<td>The maximum number of results to return at one time.</td>
</tr>
<tr>
<td>queryVersion</td>
<td>string</td>
<td>The query version.</td>
</tr>
</tbody>
</table>

Output:

```json
{
   "nextToken": "string",
   "things": [
       {
           "thingName": "string",
           "thingId": "string",
           "thingTypeName": "string",
           "thingGroupNames": [ "string" ],
           "attributes": {
               "string": "string"
           },
           "shadow": "string"
       }
   ]
}
```
**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nextToken</td>
<td>string</td>
<td>The token used to get the next set of results, or null if there are no additional results.</td>
</tr>
<tr>
<td>things</td>
<td>list</td>
<td>The things that match the search query.</td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The thing name.</td>
</tr>
<tr>
<td>thingId</td>
<td>string</td>
<td>The thing ID.</td>
</tr>
<tr>
<td>thingTypeName</td>
<td>string</td>
<td>The thing type name.</td>
</tr>
<tr>
<td>thingGroupNames</td>
<td>list</td>
<td>Thing group names.</td>
</tr>
<tr>
<td>attributes</td>
<td>map</td>
<td>The attributes.</td>
</tr>
<tr>
<td>shadow</td>
<td>string</td>
<td>The shadow.</td>
</tr>
</tbody>
</table>

**Errors:**

- **InvalidRequestException**
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ThrottlingException**
  The rate exceeds the limit.

- **UnauthorizedException**
  You are not authorized to perform this operation.

- **ServiceUnavailableException**
  The service is temporarily unavailable.

- **InternalFailureException**
  An unexpected error has occurred.

- **ResourceNotFoundException**
  The specified resource does not exist.
InvalidQueryException
The query is invalid.
IndexNotReadyException
The index is not ready.

SetDefaultAuthorizer

Sets the default authorizer. This will be used if a websocket connection is made without specifying an authorizer.

https

Request syntax:

```plaintext
POST /default-authorizer
Content-type: application/json

{
  "authorizerName": "string"
}
```

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>AuthorizerName</td>
<td>yes</td>
<td>The authorizer name.</td>
</tr>
</tbody>
</table>

Response syntax:

```plaintext
Content-type: application/json

{
  "authorizerName": "string",
  "authorizerArn": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>AuthorizerName</td>
<td>no</td>
<td>The authorizer name.</td>
</tr>
<tr>
<td>authorizerArn</td>
<td>AuthorizerArn</td>
<td>no</td>
<td>The authorizer ARN.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException
The specified resource does not exist.

HTTP response code: 404
InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an
UpdateJobExecution request contains invalid status details. The message contains details about the
error.
HTTP response code: 400
ThrottlingException
The rate exceeds the limit.
HTTP response code: 429
UnauthorizedException
You are not authorized to perform this operation.
HTTP response code: 401
ServiceUnavailableException
The service is temporarily unavailable.
HTTP response code: 503
InternalFailureException
An unexpected error has occurred.
HTTP response code: 500
ResourceAlreadyExistsException
The resource already exists.
HTTP response code: 409

cli

Synopsis:

```
aws iot set-default-authorizer \
  --authorizer-name <value> \ 
  [--cli-input-json <value>] \ 
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "authorizerName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>string</td>
<td>The authorizer name.</td>
</tr>
<tr>
<td></td>
<td>length-max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w=,@-]+</td>
<td></td>
</tr>
</tbody>
</table>
Output:

```json
{
   "authorizerName": "string",
   "authorizerArn": "string"
}
```

cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>string</td>
<td>The authorizer name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w=,@-]+</td>
<td></td>
</tr>
<tr>
<td>authorizerArn</td>
<td>string</td>
<td>The authorizer ARN.</td>
</tr>
</tbody>
</table>

Errors:

- **ResourceNotFoundException**
  - The specified resource does not exist.
- **InvalidRequestException**
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
- **ThrottlingException**
  - The rate exceeds the limit.
- **UnauthorizedException**
  - You are not authorized to perform this operation.
- **ServiceUnavailableException**
  - The service is temporarily unavailable.
- **InternalFailureException**
  - An unexpected error has occurred.
- **ResourceAlreadyExistsException**
  - The resource already exists.

**SetDefaultPolicyVersion**

Sets the specified version of the specified policy as the policy's default (operative) version. This action affects all certificates to which the policy is attached. To list the principals the policy is attached to, use the ListPrincipalPolicy API.

**https**

**Request syntax:**
PATCH /policies/{policyName}/version/{policyVersionId}

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>PolicyName</td>
<td>yes</td>
<td>The policy name.</td>
</tr>
<tr>
<td>policyVersionId</td>
<td>PolicyVersionId</td>
<td>yes</td>
<td>The policy version ID.</td>
</tr>
</tbody>
</table>

**Errors:**

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

**Synopsis:**

```
aws iot set-default-policy-version
  --policy-name <value> \
  --policy-version-id <value> \
  [--cli-input-json <value>] \
```
SetLoggingOptions

Sets the logging options.

cli-input-json format:

```
{
  "policyName": "string",
  "policyVersionId": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
<tr>
<td></td>
<td>length-</td>
<td>max:128 min:1</td>
</tr>
<tr>
<td></td>
<td>pattern:</td>
<td>[w+=,.@-]+</td>
</tr>
<tr>
<td>policyVersionId</td>
<td>string</td>
<td>The policy version ID.</td>
</tr>
<tr>
<td></td>
<td>pattern:</td>
<td>[0-9]+</td>
</tr>
</tbody>
</table>

Output:
None

Errors:

ResourceNotFoundException
The specified resource does not exist.

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException
The rate exceeds the limit.

UnauthorizedException
You are not authorized to perform this operation.

ServiceUnavailableException
The service is temporarily unavailable.

InternalFailureException
An unexpected error has occurred.
NOTE: use of this command is not recommended. Use `SetV2LoggingOptions` instead.

**Request syntax:**

```plaintext
POST /loggingOptions
Content-type: application/json

{
  "loggingOptionsPayload": {
    "roleArn": "string",
    "logLevel": "string"
  }
}
```

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>loggingOptionsPayload</td>
<td>LoggingOptionsPayload</td>
<td>yes</td>
<td>The logging options payload.</td>
</tr>
</tbody>
</table>

**Errors:**

**InternalException**

An unexpected error has occurred.

HTTP response code: 500

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an `UpdateJobExecution` request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ServiceUnavailableException**

The service is temporarily unavailable.

HTTP response code: 503

**cli**

**Synopsis:**

```bash
aws iot set-logging-options \
   --logging-options-payload <value> \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
  "loggingOptionsPayload": {
    "roleArn": "string",
    "logLevel": "string"
  }
}
```
"loggingOptionsPayload": {
   "roleArn": "string",
   "logLevel": "string"
}

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>loggingOptionsPayload</td>
<td>LoggingOptionsPayload</td>
<td>The logging options payload.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the IAM role that grants access.</td>
</tr>
<tr>
<td>logLevel</td>
<td>string</td>
<td>The log level. Enum: DEBUG</td>
</tr>
</tbody>
</table>

**Output:**

None

**Errors:**

InternalException

An unexpected error has occurred.

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ServiceUnavailableException

The service is temporarily unavailable.

---

**SetV2LoggingLevel**

Sets the logging level.

**https**

**Request syntax:**

POST /v2LoggingLevel
Content-type: application/json

{
   "logTarget": {
      "targetType": "string",
      "targetName": "string"
   },
}
"logLevel": "string"
}

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logTarget</td>
<td>LogTarget</td>
<td>yes</td>
<td>The log target.</td>
</tr>
<tr>
<td>logLevel</td>
<td>LogLevel</td>
<td>yes</td>
<td>The log level.</td>
</tr>
</tbody>
</table>

Errors:

InternalException

An unexpected error has occurred.

HTTP response code: 500

NotConfiguredException

The resource is not configured.

HTTP response code: 404

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

cli

Synopsis:

```
aws iot set-v2-logging-level 
   --log-target <value>
   --log-level <value>
   [--cli-input-json <value>]
   [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
   "logTarget": {
      "targetType": "string",
      "targetName": "string"
   },
   "logLevel": "string"
}
```
SetV2LoggingOptions

Sets the logging options for the V2 logging service.

**Request syntax:**

```
POST /v2LoggingOptions
Content-type: application/json

{
    "roleArn": "string",
    "defaultLogLevel": "string",
    "disableAllLogs": "boolean"
}
```
Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>AwsArn</td>
<td>no</td>
<td>The ARN of the role that allows IoT to write to Cloudwatch logs.</td>
</tr>
<tr>
<td>defaultLogLevel</td>
<td>LogLevel</td>
<td>no</td>
<td>The default logging level.</td>
</tr>
<tr>
<td>disableAllLogs</td>
<td>DisableAllLogs</td>
<td>no</td>
<td>If true all logs are disabled. The default is false.</td>
</tr>
</tbody>
</table>

Errors:

**InternalErrorException**

An unexpected error has occurred.

HTTP response code: 500

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ServiceUnavailableException**

The service is temporarily unavailable.

HTTP response code: 503

cli

**Synopsis:**

```
aws iot set-v2-logging-options
    [--role-arn <value>]
    [--default-log-level <value>]
    [--disable-all-logs | --no-disable-all-logs]
    [--cli-input-json <value>]
    [--generate-cli-skeleton]
```

**cli-input-json format:**

```
{
    "roleArn": "string",
    "defaultLogLevel": "string",
    "disableAllLogs": "boolean"
}
```
cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that allows IoT to write to Cloudwatch logs.</td>
</tr>
<tr>
<td>defaultLogLevel</td>
<td>string</td>
<td>The default logging level. enum: DEBUG</td>
</tr>
<tr>
<td>disableAllLogs</td>
<td>boolean</td>
<td>If true all logs are disabled. The default is false.</td>
</tr>
</tbody>
</table>

Output:
None

Errors:
- InternalException
  An unexpected error has occurred.
- InvalidRequestException
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
- ServiceUnavailableException
  The service is temporarily unavailable.

StartNextPendingJobExecution

Gets and starts the next pending (status IN_PROGRESS or QUEUED) job execution for a thing.

https

Request syntax:

```
PUT /things/thingName/jobs/$next
Content-type: application/json

{
  "statusDetails": {
    "string": "string"
  }
}
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing associated with the device.</td>
</tr>
</tbody>
</table>
Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>statusDetails</td>
<td>DetailsMap</td>
<td>no</td>
<td>A collection of name/value pairs that describe the status of the job execution. If not specified, the statusDetails are unchanged.</td>
</tr>
</tbody>
</table>

Response syntax:

```json
Content-type: application/json

{
  "execution": {
    "jobId": "string",
    "thingName": "string",
    "status": "string",
    "statusDetails": {
      "string": "string"
    },
    "queuedAt": "long",
    "startedAt": "long",
    "lastUpdatedAt": "long",
    "versionNumber": "long",
    "executionNumber": "long",
    "jobDocument": "string"
  }
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>execution</td>
<td>JobExecution</td>
<td>no</td>
<td>A JobExecution object.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429
ServiceUnavailableException
The service is temporarily unavailable.
HTTP response code: 503

CertificateValidationException
The certificate is invalid.
HTTP response code: 400

cli

Synopsis:

```
aws iot-jobs-data start-next-pending-job-execution \
  --thing-name <value> \ 
  [--status-details <value>] \ 
  [--cli-input-json <value>] \ 
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "thingName": "string",
  "statusDetails": {
    "string": "string"
  }
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing associated with the device.</td>
</tr>
<tr>
<td></td>
<td>length-</td>
<td>max:128 min:1 pattern: [a-zA-Z0-9:-_]+</td>
</tr>
<tr>
<td>statusDetails</td>
<td>map</td>
<td>A collection of name/value pairs that describe the status of the job execution. If not specified, the statusDetails are unchanged.</td>
</tr>
</tbody>
</table>

Output:

```
{
  "execution": {
    "jobId": "string",
    "thingName": "string",
    "status": "string",
    "statusDetails": {
      "string": "string"
    },
    "queuedAt": "long",
    "startedAt": "long",
    "lastUpdatedAt": "long",
    "versionNumber": "long",
```
"executionNumber": "long",
"jobDocument": "string"
}
}

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>execution</td>
<td>JobExecution</td>
<td>A JobExecution object.</td>
</tr>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier you assigned to this job when it was created.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:1</td>
<td>pattern: [a-zA-Z0-9-_]+</td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing that is executing the job.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td>pattern: [a-zA-Z0-9-_]+</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the job execution. Can be one of: &quot;QUEUED&quot;, &quot;IN_PROGRESS&quot;, &quot;FAILED&quot;, &quot;SUCCESS&quot;, &quot;CANCELED&quot;, &quot;REJECTED&quot;, or &quot;REMOVED&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: QUEUED</td>
</tr>
<tr>
<td>statusDetails</td>
<td>map</td>
<td>A collection of name/value pairs that describe the status of the job execution.</td>
</tr>
<tr>
<td>queuedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was enqueued.</td>
</tr>
<tr>
<td>startedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was started.</td>
</tr>
<tr>
<td>lastUpdatedAt</td>
<td>long</td>
<td>The time, in milliseconds since the epoch, when the job execution was last updated.</td>
</tr>
<tr>
<td>versionNumber</td>
<td>long</td>
<td>The version of the job execution. Job execution versions are incremented each time they are updated by a device.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>long</td>
<td>A number that identifies a particular job execution on a particular device. It can be used later in commands that return or update job execution information.</td>
</tr>
</tbody>
</table>
StartOnDemandAuditTask

Starts an on-demand Device Defender audit.

https

**Request syntax:**

```plaintext
POST /audit/tasks
Content-type: application/json

{
  "targetCheckNames": [
    "String"
  ]
}
```

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targetCheckNames</td>
<td>TargetAuditCheckNames</td>
<td>yes</td>
<td>Which checks are performed during the audit. The checks you specify must be enabled for your account or an exception occurs. Use</td>
</tr>
</tbody>
</table>
StartOnDemandAuditTask

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type</td>
<td>Req?</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DescribeAccountAuditConfiguration to see the list of all checks including</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>those that are enabled or UpdateAccountAuditConfiguration to select which</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>checks are enabled.</td>
</tr>
</tbody>
</table>

**Response syntax:**

Content-type: application/json

```json
{
  "taskId": "string"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>AuditTaskId</td>
<td>no</td>
<td>The ID of the on-demand audit you started.</td>
</tr>
</tbody>
</table>

**Errors:**

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

LimitExceededException

A limit has been exceeded.

HTTP response code: 410

**Synopsis:**
aws iot start-on-demand-audit-task \
   --target-check-names <value> \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]

**cli-input-json format:**

```json
{
  "targetCheckNames": [
    "string"
  ]
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targetCheckNames</td>
<td>list member: AuditCheckName</td>
<td>Which checks are performed during the audit. The checks you specify must be enabled for your account or an exception occurs. Use DescribeAccountAuditConfiguration to see the list of all checks including those that are enabled or UpdateAccountAuditConfiguration to select which checks are enabled.</td>
</tr>
</tbody>
</table>

**Output:**

```json
{
  "taskId": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>string length- max:40 min:1 pattern: [a-zA-Z0-9-]+</td>
<td>The ID of the on-demand audit you started.</td>
</tr>
</tbody>
</table>

**Errors:**

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ThrottlingException**
  
  The rate exceeds the limit.
InternalFailureException
An unexpected error has occurred.
LimitExceeded Exception
A limit has been exceeded.

StartThingRegistrationTask

Creates a bulk thing provisioning task.

https

Request syntax:

POST /thing-registration-tasks
Content-type: application/json

{
  "templateBody": "string",
  "inputFileBucket": "string",
  "inputFileKey": "string",
  "roleArn": "string"
}

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>templateBody</td>
<td>TemplateBody</td>
<td>yes</td>
<td>The provisioning template.</td>
</tr>
<tr>
<td>inputFileBucket</td>
<td>RegistryS3BucketName</td>
<td>yes</td>
<td>The S3 bucket that contains the input file.</td>
</tr>
<tr>
<td>inputFileKey</td>
<td>RegistryS3KeyName</td>
<td>yes</td>
<td>The name of input file within the S3 bucket. This file contains a newline delimited JSON file. Each line contains the parameter values to provision one device (thing).</td>
</tr>
<tr>
<td>roleArn</td>
<td>RoleArn</td>
<td>yes</td>
<td>The IAM role ARN that grants permission the input file.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{
  "taskId": "string"
}
Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>TaskId</td>
<td>no</td>
<td>The bulk thing provisioning task ID.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
HTTP response code: 400
ThrottlingException
The rate exceeds the limit.
HTTP response code: 429
UnauthorizedException
You are not authorized to perform this operation.
HTTP response code: 401
InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

cli

Synopsis:

```
aws iot start-thing-registration-task \
    --template-body <value> \
    --input-file-bucket <value> \
    --input-file-key <value> \
    --role-arn <value> \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

cli-input-json format:

```
{
    "templateBody": "string",
    "inputFileBucket": "string",
    "inputFileKey": "string",
    "roleArn": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>templateBody</td>
<td>string</td>
<td>The provisioning template.</td>
</tr>
</tbody>
</table>
### StopThingRegistrationTask

Cancels a bulk thing provisioning task.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inputFileBucket</td>
<td>string</td>
<td>The S3 bucket that contains the input file.</td>
</tr>
<tr>
<td></td>
<td>length- max:256 min:3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9_-_]+</td>
<td></td>
</tr>
<tr>
<td>inputFileKey</td>
<td>string</td>
<td>The name of input file within the S3 bucket. This file contains a newline delimited JSON file. Each line contains the parameter values to provision one device (thing).</td>
</tr>
<tr>
<td></td>
<td>length- max:1024 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9!_.*'-()-/]</td>
<td></td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The IAM role ARN that grants permission the input file.</td>
</tr>
<tr>
<td></td>
<td>length- max:2048 min:20</td>
<td></td>
</tr>
</tbody>
</table>

**Output:**

```json
{
  "taskId": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>string</td>
<td>The bulk thing provisioning task ID.</td>
</tr>
<tr>
<td></td>
<td>length- max:40</td>
<td></td>
</tr>
</tbody>
</table>

**Errors:**

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

- **ThrottlingException**
  
  The rate exceeds the limit.

- **UnauthorizedException**
  
  You are not authorized to perform this operation.

- **InternalFailureException**
  
  An unexpected error has occurred.
https

Request syntax:

```
PUT /thing-registration-tasks/<taskId>/cancel
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>TaskId</td>
<td>yes</td>
<td>The bulk thing provisioning task ID.</td>
</tr>
</tbody>
</table>

Errors:

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  
  HTTP response code: 400

- **ThrottlingException**
  
  The rate exceeds the limit.
  
  HTTP response code: 429

- **UnauthorizedException**
  
  You are not authorized to perform this operation.
  
  HTTP response code: 401

- **InternalFailureException**
  
  An unexpected error has occurred.
  
  HTTP response code: 500

- **ResourceNotFoundException**
  
  The specified resource does not exist.
  
  HTTP response code: 404

cli

Synopsis:

```
aws iot stop-thing-registration-task \
  --task-id <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:
TestAuthorization

Tests if a specified principal is authorized to perform an AWS IoT action on a specified resource. Use this to test and debug the authorization behavior of devices that connect to the AWS IoT device gateway.

https

Request syntax:

POST /test-authorization?clientId=\$\{clientId\}
Content-type: application/json

{
   "principal": "string",
   "cognitoIdentityPoolId": "string",
   "authInfos": [
   {
      "actionType": "string",
   ...

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>string</td>
<td>The bulk thing provisioning task ID.</td>
</tr>
</tbody>
</table>

Output:

None

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

InternalFailureException

An unexpected error has occurred.

ResourceNotFoundException

The specified resource does not exist.
"resources": [
  "string"
],
"policyNamesToAdd": [
  "string"
],
"policyNamesToSkip": [
  "string"
]
}

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clientId</td>
<td>ClientId</td>
<td>no</td>
<td>The MQTT client ID.</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>principal</td>
<td>Principal</td>
<td>no</td>
<td>The principal.</td>
</tr>
<tr>
<td>cognitoIdentityPoolId</td>
<td>CognitoIdentityPoolId</td>
<td>no</td>
<td>The Cognito identity pool ID.</td>
</tr>
<tr>
<td>authInfos</td>
<td>AuthInfos</td>
<td>yes</td>
<td>A list of authorization info objects. Simulating authorization will create a response for each authInfo object in the list.</td>
</tr>
<tr>
<td>policyNamesToAdd</td>
<td>PolicyNames</td>
<td>no</td>
<td>When testing custom authorization, the policies specified here are treated as if they are attached to the principal being authorized.</td>
</tr>
<tr>
<td>policyNamesToSkip</td>
<td>PolicyNames</td>
<td>no</td>
<td>When testing custom authorization, the policies specified here are treated as if they are not attached to the principal being authorized.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{
  "authResults": [
{  
    "authInfo": {  
        "actionType": "string",  
        "resources": [  
            "string"  
        ]  
    },  
    "allowed": {  
        "policies": [  
            {  
                "policyName": "string",  
                "policyArn": "string"  
            }  
        ]  
    },  
    "denied": {  
        "implicitDeny": {  
            "policies": [  
                {  
                    "policyName": "string",  
                    "policyArn": "string"  
                }  
            ]  
        },  
        "explicitDeny": {  
            "policies": [  
                {  
                    "policyName": "string",  
                    "policyArn": "string"  
                }  
            ]  
        }  
    },  
    "authDecision": "string",  
    "missingContextValues": [  
        "string"  
    ]  
}

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authResults</td>
<td>AuthResults</td>
<td>no</td>
<td>The authentication results.</td>
</tr>
</tbody>
</table>

**Errors:**

- **ResourceNotFoundException**
  
  The specified resource does not exist.
  
  HTTP response code: 404

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  
  HTTP response code: 400
ThrottlingException
The rate exceeds the limit.
HTTP response code: 429

UnauthorizedException
You are not authorized to perform this operation.
HTTP response code: 401

ServiceUnavailableException
The service is temporarily unavailable.
HTTP response code: 503

InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

LimitExceededException
A limit has been exceeded.
HTTP response code: 410

cli

Synopsis:

aws iot test-authorization \
    [--principal <value>] \
    [--cognito-identity-pool-id <value>] \
    --auth-infos <value> \
    [--client-id <value>] \
    [--policy-names-to-add <value>] \
    [--policy-names-to-skip <value>] \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]

cli-input-json format:

```json
{
    "principal": "string",
    "cognitoIdentityPoolId": "string",
    "authInfos": [
        {
            "actionType": "string",
            "resources": [
                "string"
            ]
        }
    ],
    "clientId": "string",
    "policyNamesToAdd": [
        "string"
    ],
    "policyNamesToSkip": [
        "string"
    ]
}
```
cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>principal</td>
<td>string</td>
<td>The principal.</td>
</tr>
<tr>
<td>cognitoIdentityPoolId</td>
<td>string</td>
<td>The Cognito identity pool ID.</td>
</tr>
<tr>
<td>authInfos</td>
<td>list</td>
<td>A list of authorization info objects. Simulating authorization will create a response for each authInfo object in the list.</td>
</tr>
<tr>
<td>actionType</td>
<td>string</td>
<td>The type of action for which the principal is being authorized.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: PUBLISH</td>
</tr>
<tr>
<td>resources</td>
<td>list</td>
<td>The resources for which the principal is being authorized to perform the specified action.</td>
</tr>
<tr>
<td></td>
<td>member: Resource</td>
<td></td>
</tr>
<tr>
<td>clientId</td>
<td>string</td>
<td>The MQTT client ID.</td>
</tr>
<tr>
<td>policyNamesToAdd</td>
<td>list</td>
<td>When testing custom authorization, the policies specified here are treated as if they are attached to the principal being authorized.</td>
</tr>
<tr>
<td></td>
<td>member: PolicyName</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
<tr>
<td>policyNamesToSkip</td>
<td>list</td>
<td>When testing custom authorization, the policies specified here are treated as if they are not attached to the principal being authorized.</td>
</tr>
<tr>
<td></td>
<td>member: PolicyName</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java class: java.util.List</td>
<td></td>
</tr>
</tbody>
</table>

Output:

```json
{
"authResults": [
{
  "authInfo": {
    "actionType": "string",
    "resources": [
      "string"
    ],
  },
  "allowed": {
    "policies": [
      {
        "policyName": "string",
        "policyArn": "string"
      }
    ]
  }
],
```
"denied": {  
  "implicitDeny": {  
    "policies": [  
      {  
        "policyName": "string",  
        "policyArn": "string"  
      }  
    ]  
  },  
  "explicitDeny": {  
    "policies": [  
      {  
        "policyName": "string",  
        "policyArn": "string"  
      }  
    ]  
  }  
},  
"authDecision": "string",  
"missingContextValues": [  
  "string"  
]  
]  
]  
}

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authResults</td>
<td>list</td>
<td>The authentication results.</td>
</tr>
<tr>
<td>authInfo</td>
<td>AuthInfo</td>
<td>Authorization information.</td>
</tr>
<tr>
<td>actionType</td>
<td>string</td>
<td>The type of action for which the principal is being authorized.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: PUBLISH</td>
</tr>
<tr>
<td>resources</td>
<td>list</td>
<td>The resources for which the principal is being authorized to perform the specified action.</td>
</tr>
<tr>
<td>allowed</td>
<td>Allowed</td>
<td>The policies and statements that allowed the specified action.</td>
</tr>
<tr>
<td>policies</td>
<td>list</td>
<td>A list of policies that allowed the authentication.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java class: java.util.List</td>
</tr>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>length- max:128 min:1 pattern: [w+,.@-]+</td>
</tr>
<tr>
<td>policyArn</td>
<td>string</td>
<td>The policy ARN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>denied</td>
<td>Denied</td>
<td>The policies and statements that denied the specified action.</td>
</tr>
<tr>
<td>implicitDeny</td>
<td>ImplicitDeny</td>
<td>Information that implicitly denies the authorization. When a policy doesn't explicitly deny or allow an action on a resource it is considered an implicit deny.</td>
</tr>
<tr>
<td>policies</td>
<td>list</td>
<td>Policies that don't contain a matching allow or deny statement for the specified action on the specified resource.</td>
</tr>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
<tr>
<td>policyArn</td>
<td>string</td>
<td>The policy ARN.</td>
</tr>
<tr>
<td>explicitDeny</td>
<td>ExplicitDeny</td>
<td>Information that explicitly denies the authorization.</td>
</tr>
<tr>
<td>policies</td>
<td>list</td>
<td>The policies that denied the authorization.</td>
</tr>
<tr>
<td>policyName</td>
<td>string</td>
<td>The policy name.</td>
</tr>
<tr>
<td>policyArn</td>
<td>string</td>
<td>The policy ARN.</td>
</tr>
<tr>
<td>authDecision</td>
<td>string</td>
<td>The final authorization decision of this scenario. Multiple statements are taken into account when determining the authorization decision. An explicit deny statement can override multiple allow statements.</td>
</tr>
<tr>
<td>missingContextValues</td>
<td>list</td>
<td>Contains any missing context values found while evaluating policy.</td>
</tr>
</tbody>
</table>

**Example:**

```java
import java.util.List;

public class Policy {
    private String policyName;
    private String policyArn;
    private List<Policy> policies;
}
```
TestInvokeAuthorizer

Tests a custom authorization behavior by invoking a specified custom authorizer. Use this to test and debug the custom authorization behavior of devices that connect to the AWS IoT device gateway.

https

Request syntax:

```
POST /authorizer/authorizerName/test
Content-type: application/json

{
  "token": "string",
  "tokenSignature": "string"
}
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>AuthorizerName</td>
<td>yes</td>
<td>The custom authorizer name.</td>
</tr>
</tbody>
</table>
Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>token</td>
<td>Token</td>
<td>yes</td>
<td>The token returned by your custom authentication service.</td>
</tr>
<tr>
<td>tokenSignature</td>
<td>TokenSignature</td>
<td>yes</td>
<td>The signature made with the token and your custom authentication service's private key.</td>
</tr>
</tbody>
</table>

Response syntax:

```json
Content-type: application/json
{
    "isAuthenticated": "boolean",
    "principalId": "string",
    "policyDocuments": [
        "string"
    ],
    "refreshAfterInSeconds": "integer",
    "disconnectAfterInSeconds": "integer"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>isAuthenticated</td>
<td>IsAuthenticated</td>
<td>no</td>
<td>True if the token is authenticated, otherwise false.</td>
</tr>
<tr>
<td>principalId</td>
<td>PrincipalId</td>
<td>no</td>
<td>The principal ID.</td>
</tr>
<tr>
<td>policyDocuments</td>
<td>PolicyDocuments</td>
<td>no</td>
<td>IAM policy documents.</td>
</tr>
<tr>
<td>refreshAfterInSeconds</td>
<td>Seconds</td>
<td>no</td>
<td>The number of seconds after which the temporary credentials are refreshed.</td>
</tr>
<tr>
<td>disconnectAfterSeconds</td>
<td>Seconds</td>
<td>no</td>
<td>The number of seconds after which the connection is terminated.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404
**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**UnauthorizedException**

You are not authorized to perform this operation.

HTTP response code: 401

**ServiceUnavailableException**

The service is temporarily unavailable.

HTTP response code: 503

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

**InvalidResponseException**

The response is invalid.

HTTP response code: 400

---

**cli**

**Synopsis:**

```bash
aws iot test-invoke-authorizer \
  --authorizer-name <value> \
  --token <value> \
  --token-signature <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
  "authorizerName": "string",
  "token": "string",
  "tokenSignature": "string"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>string</td>
<td>The custom authorizer name.</td>
</tr>
</tbody>
</table>
### TestInvokeAuthorizer

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>token</td>
<td>string</td>
<td>The token returned by your custom authentication service.</td>
</tr>
<tr>
<td>tokenSignature</td>
<td>string</td>
<td>The signature made with the token and your custom authentication service's private key.</td>
</tr>
</tbody>
</table>

**Output:**

```json
{
  "isAuthenticated": "boolean",
  "principalId": "string",
  "policyDocuments": [
    "string"
  ],
  "refreshAfterInSeconds": "integer",
  "disconnectAfterInSeconds": "integer"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>isAuthenticated</td>
<td>boolean</td>
<td>True if the token is authenticated, otherwise false.</td>
</tr>
<tr>
<td>principalId</td>
<td>string</td>
<td>The principal ID.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9]+</td>
<td></td>
</tr>
<tr>
<td>policyDocuments</td>
<td>list</td>
<td>IAM policy documents.</td>
</tr>
<tr>
<td></td>
<td>member: PolicyDocument</td>
<td></td>
</tr>
<tr>
<td>refreshAfterInSeconds</td>
<td>integer</td>
<td>The number of seconds after which the temporary credentials are refreshed.</td>
</tr>
<tr>
<td>disconnectAfterInSeconds</td>
<td>integer</td>
<td>The number of seconds after which the connection is terminated.</td>
</tr>
</tbody>
</table>

**Errors:**

- ResourceNotFoundException
  - The specified resource does not exist.
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

UnauthorizedException

You are not authorized to perform this operation.

ServiceUnavailableException

The service is temporarily unavailable.

InternalFailureException

An unexpected error has occurred.

InvalidResponseException

The response is invalid.

**TransferCertificate**

Transfers the specified certificate to the specified AWS account.

You can cancel the transfer until it is acknowledged by the recipient.

No notification is sent to the transfer destination's account. It is up to the caller to notify the transfer target.

The certificate being transferred must not be in the ACTIVE state. You can use the UpdateCertificate API to deactivate it.

The certificate must not have any policies attached to it. You can use the DetachPrincipalPolicy API to detach them.

**https**

**Request syntax:**

```
PATCH /transfer-certificate/certificateId?targetAwsAccount=targetAwsAccount
Content-type: application/json

{
    "transferMessage": "string"
}
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>Certificateld</td>
<td>yes</td>
<td>The ID of the certificate. (The last part of the certificate ARN contains the certificate ID.)</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Req?</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------</td>
<td>------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>targetAwsAccount</td>
<td>AwsAccountId</td>
<td>yes</td>
<td>The AWS account.</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>transferMessage</td>
<td>Message</td>
<td>no</td>
<td>The transfer message.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```json
{
  "transferredCertificateArn": "string"
}
```

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>transferredCertificateArn</td>
<td>CertificateArn</td>
<td>no</td>
<td>The ARN of the certificate.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

CertificateStateException

The certificate operation is not allowed.

HTTP response code: 406

TransferConflictException

You can't transfer the certificate because authorization policies are still attached.

HTTP response code: 409

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429
UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

/cli

Synopsis:

```
aws iot transfer-certificate \
  --certificate-id <value> \
  --target-aws-account <value> \
  [--transfer-message <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "certificateId": "string",
  "targetAwsAccount": "string",
  "transferMessage": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>string</td>
<td>The ID of the certificate. (The last part of the certificate ARN contains the certificate ID.)</td>
</tr>
<tr>
<td>targetAwsAccount</td>
<td>string</td>
<td>The AWS account.</td>
</tr>
<tr>
<td>transferMessage</td>
<td>string</td>
<td>The transfer message.</td>
</tr>
<tr>
<td></td>
<td>length- max:64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>min:64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: (0x)?[a-fA-F0-9]+</td>
<td></td>
</tr>
<tr>
<td></td>
<td>length- max:12</td>
<td></td>
</tr>
<tr>
<td></td>
<td>min:12</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [0-9]+</td>
<td></td>
</tr>
<tr>
<td></td>
<td>length- max:128</td>
<td></td>
</tr>
</tbody>
</table>

Output:
### UpdateAccountAuditConfiguration

Configures or reconfigures the Device Defender audit settings for this account. Settings include how audit notifications are sent and which audit checks are enabled or disabled.

#### https

#### Request syntax:

```shell
PATCH /audit/configuration
Content-type: application/json
```
```json
{
  "roleArn": "string",
  "auditNotificationTargetConfigurations": {
    "string": {
      "targetArn": "string",
      "roleArn": "string",
      "enabled": "boolean"
    }
  },
  "auditCheckConfigurations": {
    "string": {
      "enabled": "boolean"
    }
  }
}
```

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>RoleArn</td>
<td>no</td>
<td>The ARN of the role that grants permission to AWS IoT to access information about your devices, policies, certificates and other items as necessary when performing an audit.</td>
</tr>
<tr>
<td>auditNotificationTargetConfigurations</td>
<td>AuditNotificationTargetConfigurations</td>
<td>no</td>
<td>Information about the targets to which audit notifications are sent.</td>
</tr>
<tr>
<td>auditCheckConfigurations</td>
<td>AuditCheckConfigurations</td>
<td>no</td>
<td>Specifies which audit checks are enabled and disabled for this account. Use DescribeAccountAuditConfiguration to see the list of all checks including those that are currently enabled. Note that some data collection may begin immediately when certain checks are enabled. When a check is disabled, any data collected so far in relation to the check is deleted. You cannot disable a check if it is used by any scheduled audit. You must first delete the check from the account.</td>
</tr>
</tbody>
</table>
UpdateAccountAuditConfiguration

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>scheduled audit or delete the scheduled audit itself.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>On the first call to UpdateAccountAuditConfiguration this parameter is</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>required and must specify at least one enabled check.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot update-account-audit-configuration \
  [--role-arn <value>] \
  [--audit-notification-target-configurations <value>] \
  [--audit-check-configurations <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "roleArn": "string",
  "auditNotificationTargetConfigurations": {
    "string": {
      "targetArn": "string",
      "roleArn": "string",
      "enabled": "boolean"
    }
  },
  "auditCheckConfigurations": {
    "string": {
      "enabled": "boolean"
    }
  }
}
```
### cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants permission to AWS IoT to access information about your devices, policies, certificates and other items as necessary when performing an audit.</td>
</tr>
<tr>
<td></td>
<td>length- max:2048 min:20</td>
<td></td>
</tr>
<tr>
<td>auditNotificationTargetConfigurations</td>
<td>map</td>
<td>Information about the targets to which audit notifications are sent.</td>
</tr>
<tr>
<td>targetArn</td>
<td>string</td>
<td>The ARN of the target (SNS topic) to which audit notifications are sent.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants permission to send notifications to the target.</td>
</tr>
<tr>
<td></td>
<td>length- max:2048 min:20</td>
<td></td>
</tr>
<tr>
<td>enabled</td>
<td>boolean</td>
<td>True if notifications to the target are enabled.</td>
</tr>
<tr>
<td>auditCheckConfigurations</td>
<td>map</td>
<td>Specifies which audit checks are enabled and disabled for this account. Use DescribeAccountAuditConfiguration to see the list of all checks including those that are currently enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note that some data collection may begin immediately when certain checks are enabled. When a check is disabled, any data collected so far in relation to the check is deleted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You cannot disable a check if it is used by any scheduled audit. You must first delete the check from the scheduled audit or delete the scheduled audit itself.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On the first call to UpdateAccountAuditConfiguration this parameter is required and must specify at least one enabled check.</td>
</tr>
<tr>
<td>enabled</td>
<td>boolean</td>
<td>True if this audit check is enabled for this account.</td>
</tr>
</tbody>
</table>
Output:
None

Errors:
InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
ThrottlingException
The rate exceeds the limit.
InternalFailureException
An unexpected error has occurred.

UpdateAuthorizer

Updates an authorizer.

https

Request syntax:

```
PUT /authorizer/authorizerName
Content-type: application/json

{
  "authorizerFunctionArn": "string",
  "tokenKeyName": "string",
  "tokenSigningPublicKeys": {
    "string": "string"
  },
  "status": "string"
}
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>AuthorizerName</td>
<td>yes</td>
<td>The authorizer name.</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerFunctionArn</td>
<td>AuthorizerFunctionArn</td>
<td>no</td>
<td>The ARN of the authorizer's Lambda function.</td>
</tr>
<tr>
<td>tokenKeyName</td>
<td>TokenKeyName</td>
<td>no</td>
<td>The key used to extract the token from the HTTP headers.</td>
</tr>
</tbody>
</table>
### Name | Type | Req? | Description
--- | --- | --- | ---
tokenSigningPublicKeys | PublicKeyMap | no | The public keys used to verify the token signature.
status | AuthorizerStatus | no | The status of the update authorizer request.

**Response syntax:**

```
Content-type: application/json
{
  "authorizerName": "string",
  "authorizerArn": "string"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>AuthorizerName</td>
<td>no</td>
<td>The authorizer name.</td>
</tr>
<tr>
<td>authorizerArn</td>
<td>AuthorizerArn</td>
<td>no</td>
<td>The authorizer ARN.</td>
</tr>
</tbody>
</table>

**Errors:**

<ResourceNotFoundException>

The specified resource does not exist.

HTTP response code: 404

<InvalidRequestException>

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

<LimitExceededException>

A limit has been exceeded.

HTTP response code: 410

<ThrottlingException>

The rate exceeds the limit.

HTTP response code: 429

<UnauthorizedException>

You are not authorized to perform this operation.

HTTP response code: 401
ServiceUnavailableException

The service is temporarily unavailable.
HTTP response code: 503

InternalFailureException

An unexpected error has occurred.
HTTP response code: 500

cli

Synopsis:

```sh
aws iot update-authorizer \
  --authorizer-name <value> \
  [--authorizer-function-arn <value>] \
  [--token-key-name <value>] \
  [--token-signing-public-keys <value>] \
  [--status <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "authorizerName": "string",
  "authorizerFunctionArn": "string",
  "tokenKeyName": "string",
  "tokenSigningPublicKeys": {
    "string": "string"
  },
  "status": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorizerName</td>
<td>string</td>
<td>The authorizer name.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [w=,@-]+</td>
<td></td>
</tr>
<tr>
<td>authorizerFunctionArn</td>
<td>string</td>
<td>The ARN of the authorizer's Lambda function.</td>
</tr>
<tr>
<td>tokenKeyName</td>
<td>string</td>
<td>The key used to extract the token from the HTTP headers.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9_-]+</td>
<td></td>
</tr>
<tr>
<td>tokenSigningPublicKeys</td>
<td>map</td>
<td>The public keys used to verify the token signature.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the update authorizer request.</td>
</tr>
</tbody>
</table>
**UpdateCACertificate**

Updates a registered CA certificate.

**https**

**Request syntax:**
**PUT /cacertificate/caCertificateId?**
newStatus=newStatus&newAutoRegistrationStatus=newAutoRegistrationStatus
Content-type: application/json

```json
{
  "registrationConfig": {
    "templateBody": "string",
    "roleArn": "string"
  },
  "removeAutoRegistration": "boolean"
}
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>CertificateId</td>
<td>yes</td>
<td>The CA certificate identifier.</td>
</tr>
<tr>
<td>newStatus</td>
<td>CACertificateStatus</td>
<td>no</td>
<td>The updated status of the CA certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> The status value REGISTER_INACTIVE is deprecated and should not be used.</td>
</tr>
<tr>
<td>newAutoRegistrationStatus</td>
<td>AutoRegistrationStatus</td>
<td>no</td>
<td>The new value for the auto registration status. Valid values: &quot;ENABLE&quot; or &quot;DISABLE&quot;.</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>registrationConfig</td>
<td>RegistrationConfig</td>
<td>no</td>
<td>Information about the registration configuration.</td>
</tr>
<tr>
<td>removeAutoRegistration</td>
<td>RemoveAutoRegistration</td>
<td>no</td>
<td>If true, remove auto registration.</td>
</tr>
</tbody>
</table>

**Errors:**

- **ResourceNotFoundException**
  The specified resource does not exist.
  HTTP response code: 404

- **InvalidRequestException**
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  HTTP response code: 400
ThrottlingException
The rate exceeds the limit.
HTTP response code: 429

UnauthorizedException
You are not authorized to perform this operation.
HTTP response code: 401

ServiceUnavailableException
The service is temporarily unavailable.
HTTP response code: 503

InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

cli

Synopsis:

```
aws iot update-ca-certificate
   --certificate-id <value> \
   [--new-status <value>] \
   [--new-auto-registration-status <value>] \
   [--registration-config <value>] \
   [--remove-auto-registration | --no-remove-auto-registration] \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "certificateId": "string",
   "newStatus": "string",
   "newAutoRegistrationStatus": "string",
   "registrationConfig": {
      "templateBody": "string",
      "roleArn": "string"
   },
   "removeAutoRegistration": "boolean"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>string</td>
<td>The CA certificate identifier.</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:64 pattern: (0x)?[a-fA-F0-9]+</td>
<td></td>
</tr>
<tr>
<td>newStatus</td>
<td>string</td>
<td>The updated status of the CA certificate.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The status value REGISTER_INACTIVE is deprecated and should not be used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: ACTIVE</td>
</tr>
<tr>
<td>newAutoRegistrationStatus</td>
<td>string</td>
<td>The new value for the auto registration status. Valid values are: &quot;ENABLE&quot; or &quot;DISABLE&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: ENABLE</td>
</tr>
<tr>
<td>registrationConfig</td>
<td>RegistrationConfig</td>
<td>Information about the registration configuration.</td>
</tr>
<tr>
<td>templateBody</td>
<td>string</td>
<td>The template body.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>length- max:2048 min:20</td>
</tr>
<tr>
<td>removeAutoRegistration</td>
<td>boolean</td>
<td>If true, remove auto registration.</td>
</tr>
</tbody>
</table>

Output:
None

Errors:

ResourceNotFoundException
The specified resource does not exist.

InvalidRequestException
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException
The rate exceeds the limit.

UnauthorizedException
You are not authorized to perform this operation.

ServiceUnavailableException
The service is temporarily unavailable.

InternalFailureException
An unexpected error has occurred.

**UpdateCertificate**
Updates the status of the specified certificate. This operation is idempotent.
Moving a certificate from the ACTIVE state (including REVOKED) will not disconnect currently connected devices, but these devices will be unable to reconnect.

The ACTIVE state is required to authenticate devices connecting to AWS IoT using a certificate.

**https**

**Request syntax:**

```plaintext
PUT /certificates/certificateId?newStatus=newStatus
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>CertificateId</td>
<td>yes</td>
<td>The ID of the certificate. (The last part of the certificate ARN contains the certificate ID.)</td>
</tr>
<tr>
<td>newStatus</td>
<td>CertificateStatus</td>
<td>yes</td>
<td>The new status.</td>
</tr>
</tbody>
</table>

**Note:** Setting the status to PENDING_TRANSFER will result in an exception being thrown. PENDING_TRANSFER is a status used internally by AWS IoT. It is not intended for developer use.

**Note:** The status value REGISTER_INACTIVE is deprecated and should not be used.

**Errors:**

- **ResourceNotFoundException**
  
  The specified resource does not exist.
  
  HTTP response code: 404

- **CertificateStateException**
  
  The certificate operation is not allowed.
  
  HTTP response code: 406

- **InvalidRequestException**
  
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  
  HTTP response code: 400
ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot update-certificate \
  --certificate-id <value> \
  --new-status <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "certificateId": "string",
  "newStatus": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificateId</td>
<td>string</td>
<td>The ID of the certificate. (The last part of the certificate ARN contains the certificate ID.)</td>
</tr>
<tr>
<td></td>
<td>length- max:64 min:64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: (0x)[a-fA-F0-9]+</td>
<td></td>
</tr>
<tr>
<td>newStatus</td>
<td>string</td>
<td>The new status.</td>
</tr>
</tbody>
</table>

Note: Setting the status to PENDING_TRANSFER will result in an exception being thrown. PENDING_TRANSFER is a status used internally by AWS IoT. It is not intended for developer use.
UpdateEventConfigurations

Updates the event configurations.

https

Request syntax:

PATCH /event-configurations

### Name | Type | Description
--- | --- | ---

- **Note:** The status value `REGISTER_INACTIVE` is deprecated and should not be used.
- `enum: ACTIVE | INACTIVE | REVOKED | PENDING_TRANSFER | REGISTER_INACTIVE | PENDING_ACTIVATION`

Output:

None

Errors:

- **ResourceNotFoundException**
  - The specified resource does not exist.
- **CertificateStateException**
  - The certificate operation is not allowed.
- **InvalidRequestException**
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
- **ThrottlingException**
  - The rate exceeds the limit.
- **UnauthorizedException**
  - You are not authorized to perform this operation.
- **ServiceUnavailableException**
  - The service is temporarily unavailable.
- **InternalFailureException**
  - An unexpected error has occurred.
Content-type: application/json

{
   "eventConfigurations": {
      "string": {
         "Enabled": "boolean"
      }
   }
}

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventConfigurations</td>
<td>EventConfigurations</td>
<td>no</td>
<td>The new event configuration values.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

cli

Synopsis:

```
aws iot update-event-configurations \[-event-configurations <value>] \[-cli-input-json <value>] \[-generate-cli-skeleton]
```

cli-input-json format:

```
{
   "eventConfigurations": {
      "string": {
         "Enabled": "boolean"
      }
   }
}
```
**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventConfigurations</td>
<td>map</td>
<td>The new event configuration values.</td>
</tr>
<tr>
<td>Enabled</td>
<td>boolean</td>
<td>True to enable the configuration.</td>
</tr>
</tbody>
</table>

**Output:**

None

**Errors:**

`InvalidRequestException`

The contents of the request were invalid. For example, this code is returned when an `UpdateJobExecution` request contains invalid status details. The message contains details about the error.

`InternalFailureException`

An unexpected error has occurred.

`ThrottlingException`

The rate exceeds the limit.

---

**UpdateIndexingConfiguration**

Updates the search configuration.

**https**

**Request syntax:**

```
POST /indexing/config
Content-type: application/json

{
  "thingIndexingConfiguration": {
    "thingIndexingMode": "string"
  }
}
```

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingIndexingConfiguration</td>
<td>thingIndexingConfiguration</td>
<td></td>
<td>Thing indexing configuration.</td>
</tr>
</tbody>
</table>

**Errors:**

1083
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot update-indexing-configuration \
    [--thing-indexing-configuration <value>] \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

cli-input-json format:

```
{
    "thingIndexingConfiguration": {
        "thingIndexingMode": "String"
    }
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingIndexingConfiguration</td>
<td>ThingIndexingConfiguration</td>
<td>Thing indexing configuration.</td>
</tr>
<tr>
<td>thingIndexingMode</td>
<td>string</td>
<td>Thing indexing mode. Valid values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• REGISTRY – Your thing index will contain only registry data.</td>
</tr>
</tbody>
</table>
UpdateJobExecution

Updates the status of a job execution.

**https**

**Request syntax:**

```json
POST /things/thingName/jobs/jobId
Content-type: application/json

{
  "status": "string",
  "statusDetails": {
    "string": "string"
  },
  "expectedVersion": "long",
```
"includeJobExecutionState": "boolean",
"includeJobDocument": "boolean",
"executionNumber": "long"
}

### URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>JobId</td>
<td>yes</td>
<td>The unique identifier assigned to this job when it was created.</td>
</tr>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing associated with the device.</td>
</tr>
</tbody>
</table>

### Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>JobExecutionStatus</td>
<td>yes</td>
<td>The new status for the job execution (IN_PROGRESS, FAILED, SUCCESS, or REJECTED). This must be specified on every update.</td>
</tr>
<tr>
<td>statusDetails</td>
<td>DetailsMap</td>
<td>no</td>
<td>Optional. A collection of name/value pairs that describe the status of the job execution. If not specified, the statusDetails are unchanged.</td>
</tr>
<tr>
<td>expectedVersion</td>
<td>ExpectedVersion</td>
<td>no</td>
<td>Optional. The expected current version of the job execution. Each time you update the job execution, its version is incremented. If the version of the job execution stored in Jobs does not match, the update is rejected with a VersionMismatch error, and an ErrorResponse that contains the current job execution status data is returned. (This makes it unnecessary to perform a separate DescribeJobExecution request in order</td>
</tr>
</tbody>
</table>
AWS IoT Developer Guide
UpdateJobExecution

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>includeJobExecutionState</td>
<td>IncludeExecutionState</td>
<td>no</td>
<td>Optional. When included and set to true, the response contains the JobExecutionState data. The default is false.</td>
</tr>
<tr>
<td>includeJobDocument</td>
<td>IncludeJobDocument</td>
<td>no</td>
<td>Optional. When set to true, the response contains the job document. The default is false.</td>
</tr>
<tr>
<td>executionNumber</td>
<td>ExecutionNumber</td>
<td>no</td>
<td>Optional. A number that identifies a particular job execution on a particular device.</td>
</tr>
</tbody>
</table>

**Response syntax:**

```json
Content-type: application/json
{
    "executionState": {
        "status": "string",
        "statusDetails": {
            "string": "string"
        },
        "versionNumber": "long"
    },
    "jobDocument": "string"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>executionState</td>
<td>JobExecutionState</td>
<td>no</td>
<td>A JobExecutionState object.</td>
</tr>
<tr>
<td>jobDocument</td>
<td>JobDocument</td>
<td>no</td>
<td>The contents of the Job Documents.</td>
</tr>
</tbody>
</table>

**Errors:**

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400
ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

CertificateValidationException

The certificate is invalid.

HTTP response code: 400

InvalidStateTransitionException

An update attempted to change the job execution to a state that is invalid because of the job execution's current state (for example, an attempt to change a request in state SUCCESS to state IN_PROGRESS). In this case, the body of the error message also contains the executionState field.

HTTP response code: 409

cli

Synopsis:

```
aws iot-jobs-data update-job-execution
--job-id <value> \
--thing-name <value> \ 
--status <value> \ 
[--status-details <value>] \ 
[--expected-version <value>] \ 
[--include-job-execution-state | --no-include-job-execution-state] \ 
[--include-job-document | --no-include-job-document] \ 
[--execution-number <value>] \ 
[--cli-input-json <value>] \ 
[--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "jobId": "string",
  "thingName": "string",
  "status": "string",
  "statusDetails": {
    "string": "string"
  },
  "expectedVersion": "long",
  "includeJobExecutionState": "boolean",
  "includeJobDocument": "boolean",
  "executionNumber": "long"
}
```
### cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobId</td>
<td>string</td>
<td>The unique identifier assigned to this job when it was created.</td>
</tr>
<tr>
<td>length- max:64 min:1 pattern: [a-zA-Z0-9-_]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing associated with the device.</td>
</tr>
<tr>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9:_-_]+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The new status for the job execution (IN_PROGRESS, FAILED, SUCCESS, or REJECTED). This must be specified on every update.</td>
</tr>
<tr>
<td>enum: QUEUED</td>
<td>IN_PROGRESS</td>
<td>SUCCEEDED</td>
</tr>
<tr>
<td>statusDetails</td>
<td>map</td>
<td>Optional. A collection of name/value pairs that describe the status of the job execution. If not specified, the statusDetails are unchanged.</td>
</tr>
<tr>
<td>expectedVersion</td>
<td>long</td>
<td>Optional. The expected current version of the job execution. Each time you update the job execution, its version is incremented. If the version of the job execution stored in Jobs does not match, the update is rejected with a VersionMismatch error, and an ErrorResponse that contains the current job execution status data is returned. (This makes it unnecessary to perform a separate DescribeJobExecution request in order to obtain the job execution status data.)</td>
</tr>
<tr>
<td>includeJobExecutionState</td>
<td>boolean</td>
<td>Optional. When included and set to true, the response contains the JobExecutionState data. The default is false.</td>
</tr>
<tr>
<td>includeJobDocument</td>
<td>boolean</td>
<td>Optional. When set to true, the response contains the job document. The default is false.</td>
</tr>
</tbody>
</table>
## Name | Type | Description
--- | --- | ---
executionNumber | long | Optional. A number that identifies a particular job execution on a particular device.

### Output:

```json
{
  "executionState": {
    "status": "string",
    "statusDetails": {
      "string": "string"
    },
    "versionNumber": "long"
  },
  "jobDocument": "string"
}
```

### cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>executionState</td>
<td>JobExecutionState</td>
<td>A JobExecutionState object.</td>
</tr>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the job execution. Can be one of: &quot;QUEUED&quot;, &quot;IN_PROGRESS&quot;, &quot;FAILED&quot;, &quot;SUCCESS&quot;, &quot;CANCELED&quot;, &quot;REJECTED&quot;, or &quot;REMOVED&quot;. enum: QUEUED</td>
</tr>
<tr>
<td>statusDetails</td>
<td>map</td>
<td>A collection of name/value pairs that describe the status of the job execution.</td>
</tr>
<tr>
<td>versionNumber</td>
<td>long</td>
<td>The version of the job execution. Job execution versions are incremented each time they are updated by a device.</td>
</tr>
<tr>
<td>jobDocument</td>
<td>string</td>
<td>The contents of the Job Documents.</td>
</tr>
<tr>
<td>length- max:32768</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Errors:

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

**ResourceNotFoundException**

The specified resource does not exist.
ThrottlingException
- The rate exceeds the limit.

ServiceUnavailableException
- The service is temporarily unavailable.

CertificateValidationException
- The certificate is invalid.

InvalidStateTransitionException
- An update attempted to change the job execution to a state that is invalid because of the job execution's current state (for example, an attempt to change a request in state SUCCESS to state IN_PROGRESS). In this case, the body of the error message also contains the executionState field.

UpdateRoleAlias

Updates a role alias.

https

Request syntax:

PUT /role-aliases/roleAlias
Content-type: application/json

{
  "roleArn": "string",
  "credentialDurationSeconds": "integer"
}

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleAlias</td>
<td>RoleAlias</td>
<td>yes</td>
<td>The role alias to update.</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleArn</td>
<td>RoleArn</td>
<td>no</td>
<td>The role ARN.</td>
</tr>
<tr>
<td>credentialDurationSeconds</td>
<td>CredentialDurationSeconds</td>
<td>no</td>
<td>The number of seconds the credential will be valid.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{
  "roleAlias": "string",
  "roleAliasArn": "string"
}
Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleAlias</td>
<td>RoleAlias</td>
<td>no</td>
<td>The role alias.</td>
</tr>
<tr>
<td>roleAliasArn</td>
<td>RoleAliasArn</td>
<td>no</td>
<td>The role alias ARN.</td>
</tr>
</tbody>
</table>

Errors:

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

UnauthorizedException

You are not authorized to perform this operation.

HTTP response code: 401

ServiceUnavailableException

The service is temporarily unavailable.

HTTP response code: 503

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot update-role-alias \
  --role-alias <value> \
  [--role-arn <value>] \
  [--credential-duration-seconds <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:
UpdateRoleAlias

```json
{
  "roleAlias": "string",
  "roleArn": "string",
  "credentialDurationSeconds": "integer"
}
```

**cli-input-json fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleAlias</td>
<td>string</td>
<td>The role alias to update.</td>
</tr>
<tr>
<td></td>
<td>length-</td>
<td>max:128 min:1</td>
</tr>
<tr>
<td></td>
<td>pattern: [w=,@-]+</td>
<td></td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The role ARN.</td>
</tr>
<tr>
<td></td>
<td>length-</td>
<td>max:2048 min:20</td>
</tr>
<tr>
<td>credentialDurationSeconds</td>
<td>integer</td>
<td>The number of seconds the credential will be valid.</td>
</tr>
<tr>
<td></td>
<td>range-</td>
<td>max:3600 min:900</td>
</tr>
</tbody>
</table>

**Output:**

```json
{
  "roleAlias": "string",
  "roleAliasArn": "string"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roleAlias</td>
<td>string</td>
<td>The role alias.</td>
</tr>
<tr>
<td></td>
<td>length-</td>
<td>max:128 min:1</td>
</tr>
<tr>
<td></td>
<td>pattern: [w=,@-]+</td>
<td></td>
</tr>
<tr>
<td>roleAliasArn</td>
<td>string</td>
<td>The role alias ARN.</td>
</tr>
</tbody>
</table>

**Errors:**

**ResourceNotFoundException**

The specified resource does not exist.

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

**ThrottlingException**

The rate exceeds the limit.
UpdateScheduledAudit

Updates a scheduled audit, including what checks are performed and how often the audit takes place.

https

Request syntax:

```
PATCH /audit/scheduledaudits/scheduledAuditName
Content-type: application/json

{  
  "frequency": "string",
  "dayOfMonth": "string",
  "dayOfWeek": "string",
  "targetCheckNames": [  
    "string"
  ]
}
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditName</td>
<td>ScheduledAuditName</td>
<td>yes</td>
<td>The name of the scheduled audit. (Max. 128 chars)</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>AuditFrequency</td>
<td>no</td>
<td>How often the scheduled audit takes place. Can be one of &quot;DAILY&quot;, &quot;WEEKLY&quot;,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;BIWEEKLY&quot; or &quot;MONTHLY&quot;. The actual start time of each audit is determined</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>by the system.</td>
</tr>
<tr>
<td>dayOfMonth</td>
<td>DayOfMonth</td>
<td>no</td>
<td>The day of the month on which the scheduled audit takes place. Can be &quot;1&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>through 1094.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Req?</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------</td>
<td>------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| dayOfWeek          | DayOfWeek          | no   | The day of the week on which the scheduled audit takes place. Can be one of "SUN", "MON", "TUE", "WED", "THU", "FRI" or "SAT". This field is required if the "frequency" parameter is set to "WEEKLY" or "BIWEEKLY".
| targetCheckNames   | TargetAuditCheckNames | no   | Which checks are performed during the scheduled audit. Checks must be enabled for your account. (Use DescribeAccountAuditConfiguration to see the list of all checks including those that are enabled or UpdateAccountAuditConfiguration to select which checks are enabled.)                                                                                           |

**Response syntax:**

```json
Content-type: application/json

{
  "scheduledAuditArn": "string"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditArn</td>
<td>ScheduledAuditArn</td>
<td>no</td>
<td>The ARN of the scheduled audit.</td>
</tr>
</tbody>
</table>

**Errors:**
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an
UpdateJobExecution request contains invalid status details. The message contains details about the
error.

HTTP response code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot update-scheduled-audit \
   [--frequency <value>] \
   [--day-of-month <value>] \
   [--day-of-week <value>] \
   [--target-check-names <value>] \
   --scheduled-audit-name <value>  \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
   "frequency": "string",
   "dayOfMonth": "string",
   "dayOfWeek": "string",
   "targetCheckNames": [ 
      "string"
   ],
   "scheduledAuditName": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>string</td>
<td>How often the scheduled audit takes place. Can be one of &quot;DAILY&quot;, &quot;WEEKLY&quot;, &quot;BIWEEKLY&quot; or &quot;MONTHLY&quot;. The actual start time of each audit is determined by the system.</td>
</tr>
</tbody>
</table>
### Name | Type | Description
---|---|---
| **scheduledAuditArn** | **string** | The ARN of the scheduled audit. |

### Output:

```
{
  "scheduledAuditArn": "string"
}
```

### cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduledAuditArn</td>
<td>string</td>
<td>The ARN of the scheduled audit.</td>
</tr>
</tbody>
</table>
UpdateSecurityProfile

Updates a Device Defender security profile.

https

Request syntax:

```plaintext
PATCH /security-profiles/securityProfileName?expectedVersion=expectedVersion
Content-type: application/json

{
  "securityProfileDescription": "string",
  "behaviors": [
    {
      "name": "string",
      "metric": "string",
      "criteria": {
        "comparisonOperator": "string",
        "value": {
          "count": "long",
          "cidrs": ["string"],
          "ports": [
            "integer"
          ],
          "durationSeconds": "integer"
        }
      }
    },
    "alertTargets": {
      "string": {
        "alertTargetArn": "string",
        "roleArn": "string"
      }
    }
  }
}
```
URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>yes</td>
<td>The name of the security profile you want to update.</td>
</tr>
<tr>
<td>expectedVersion</td>
<td>OptionalVersion</td>
<td>no</td>
<td>The expected version of the security profile. A new version is generated whenever the security profile is updated. If you specify a value that is different than the actual version, a VersionConflictException is thrown.</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileDescription</td>
<td>SecurityProfileDescription</td>
<td>no</td>
<td>A description of the security profile.</td>
</tr>
<tr>
<td>behaviors</td>
<td>Behaviors</td>
<td>no</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td>alertTargets</td>
<td>AlertTargets</td>
<td>no</td>
<td>Where the alerts are sent. (Alerts are always sent to the console.)</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

```json
{
  "securityProfileName": "string",
  "securityProfileArn": "string",
  "securityProfileDescription": "string",
  "behaviors": [
    {
      "name": "string",
      "metric": "string",
      "criteria": {
        "comparisonOperator": "string",
        "value": {
          "count": "long",
          "cidrs": [
            "string"
          ],
          "ports": [
            "integer"
          ]
```
Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>SecurityProfileName</td>
<td>no</td>
<td>The name of the security profile that was updated.</td>
</tr>
<tr>
<td>securityProfileArn</td>
<td>SecurityProfileArn</td>
<td>no</td>
<td>The ARN of the security profile that was updated.</td>
</tr>
<tr>
<td>securityProfileDescription</td>
<td>SecurityProfileDescription</td>
<td>no</td>
<td>The description of the security profile.</td>
</tr>
<tr>
<td>behaviors</td>
<td>Behaviors</td>
<td>no</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td>alertTargets</td>
<td>AlertTargets</td>
<td>no</td>
<td>Where the alerts are sent. (Alerts are always sent to the console.)</td>
</tr>
<tr>
<td>version</td>
<td>Version</td>
<td>no</td>
<td>The updated version of the security profile.</td>
</tr>
<tr>
<td>creationDate</td>
<td>Timestamp</td>
<td>no</td>
<td>The time the security profile was created.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>Timestamp</td>
<td>no</td>
<td>The time the security profile was last modified.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400
ResourceNotFoundException
The specified resource does not exist.
HTTP response code: 404

VersionConflictException
An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.
HTTP response code: 409

ThrottlingException
The rate exceeds the limit.
HTTP response code: 429

InternalFailureException
An unexpected error has occurred.
HTTP response code: 500

cli

Synopsis:

```
aws iot update-security-profile \
   --security-profile-name <value> \
   [--security-profile-description <value>] \
   [--behaviors <value>] \
   [--alert-targets <value>] \
   [--expected-version <value>] \
   [--cli-input-json <value>] \
   [--generate-cli-skeleton]
```

cli-input-json format:

```
{
    "securityProfileName": "string",
    "securityProfileDescription": "string",
    "behaviors": [
      {
        "name": "string",
        "metric": "string",
        "criteria": {
          "comparisonOperator": "string",
          "value": {
            "count": "long",
            "cidrs": ["string"],
            "ports": ["integer"],
          }
        },
        "durationSeconds": "integer"
      }
    ],
    "alertTargets": {
      "string": {
      }
    }
}
```
cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name of the security profile you want to update.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>securityProfileDescription</td>
<td>string</td>
<td>A description of the security profile.</td>
</tr>
<tr>
<td></td>
<td>length- max:1000 pattern: [\p{Graph}]*</td>
<td></td>
</tr>
<tr>
<td>behaviors</td>
<td>list member: Behavior</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the behavior.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>metric</td>
<td>string</td>
<td>What is measured by the behavior.</td>
</tr>
<tr>
<td>criteria</td>
<td>BehaviorCriteria</td>
<td>The criteria that determine if a device is behaving normally in regard to the metric.</td>
</tr>
<tr>
<td>comparisonOperator</td>
<td>string</td>
<td>The operator that relates the thing measured (metric) to the criteria (value). enum: less-than</td>
</tr>
<tr>
<td>value</td>
<td>MetricValue</td>
<td>The value to be compared with the metric.</td>
</tr>
<tr>
<td>count</td>
<td>long</td>
<td>If the comparisonOperator calls for a numeric value, use this to specify that numeric value to be compared with the metric. range- min:0</td>
</tr>
<tr>
<td>cidrs</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of CIDRs, use</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>name</td>
<td>member: Cidr</td>
<td>this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>ports</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of ports, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>durationSeconds</td>
<td>integer</td>
<td>Use this to specify the period of time over which the behavior is evaluated, for those criteria which have a time dimension (for example, NUM_MESSAGES_SENT).</td>
</tr>
<tr>
<td>alertTargets</td>
<td>map</td>
<td>Where the alerts are sent. (Alerts are always sent to the console.)</td>
</tr>
<tr>
<td>alertTargetArn</td>
<td>string</td>
<td>The ARN of the notification target to which alerts are sent.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants permission to send alerts to the notification target.</td>
</tr>
<tr>
<td>expectedVersion</td>
<td>long</td>
<td>The expected version of the security profile. A new version is generated whenever the security profile is updated. If you specify a value that is different than the actual version, a VersionConflictException is thrown.</td>
</tr>
</tbody>
</table>

Output:

```json
{
  "securityProfileName": "string",
  "securityProfileArn": "string",
  "securityProfileDescription": "string",
  "behaviors": [
    {
      "name": "string",
      "metric": "string",
      "criteria": {
        "comparisonOperator": "string",
        "value": {
          "count": "long",
          "cidrs": [
            "string"
          ],
          "ports": [
            "integer"
          ]
        },
        "durationSeconds": "integer"
      }
    }
  ]
}
```
cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityProfileName</td>
<td>string</td>
<td>The name of the security profile that was updated.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>securityProfileArn</td>
<td>string</td>
<td>The ARN of the security profile that was updated.</td>
</tr>
<tr>
<td>securityProfileDescription</td>
<td>string</td>
<td>The description of the security profile.</td>
</tr>
<tr>
<td></td>
<td>length- max:1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [\p{Graph}]*</td>
<td></td>
</tr>
<tr>
<td>behaviors</td>
<td>list</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the behavior.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>metric</td>
<td>string</td>
<td>What is measured by the behavior.</td>
</tr>
<tr>
<td>criteria</td>
<td>BehaviorCriteria</td>
<td>The criteria that determine if a device is behaving normally in regard to the metric.</td>
</tr>
<tr>
<td>comparisonOperator</td>
<td>string</td>
<td>The operator that relates the thing measured (metric) to the criteria (value).</td>
</tr>
<tr>
<td></td>
<td>enum: less-than</td>
<td>less-than-equals</td>
</tr>
<tr>
<td>value</td>
<td>MetricValue</td>
<td>The value to be compared with the metric.</td>
</tr>
</tbody>
</table>
## UpdateSecurityProfile

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>long</td>
<td>If the comparisonOperator calls for a numeric value, use this to specify that numeric value to be compared with the metric.</td>
</tr>
<tr>
<td>cidrs</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of CIDRs, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>ports</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of ports, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td>durationSeconds</td>
<td>integer</td>
<td>Use this to specify the period of time over which the behavior is evaluated, for those criteria which have a time dimension (for example, NUM_MESSAGES_SENT).</td>
</tr>
<tr>
<td>alertTargets</td>
<td>map</td>
<td>Where the alerts are sent. (Alerts are always sent to the console.)</td>
</tr>
<tr>
<td>alertTargetArn</td>
<td>string</td>
<td>The ARN of the notification target to which alerts are sent.</td>
</tr>
<tr>
<td>roleArn</td>
<td>string</td>
<td>The ARN of the role that grants permission to send alerts to the notification target.</td>
</tr>
<tr>
<td>version</td>
<td>long</td>
<td>The updated version of the security profile.</td>
</tr>
<tr>
<td>creationDate</td>
<td>timestamp</td>
<td>The time the security profile was created.</td>
</tr>
<tr>
<td>lastModifiedDate</td>
<td>timestamp</td>
<td>The time the security profile was last modified.</td>
</tr>
</tbody>
</table>

### Errors:

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

**ResourceNotFoundException**

The specified resource does not exist.

**VersionConflictException**

An exception thrown when the version of a thing passed to a command is different than the version specified with the `--version` parameter.
ThrottlingException
  The rate exceeds the limit.
InternalFailureException
  An unexpected error has occurred.

**UpdateStream**

Updates an existing stream. The stream version will be incremented by one.

**https**

**Request syntax:**

```
PUT /streams/streamId
Content-type: application/json

{
  "description": "string",
  "files": [
    {
      "fileId": "integer",
      "s3Location": {
        "bucket": "string",
        "key": "string",
        "version": "string"
      }
    }
  ],
  "roleArn": "string"
}
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streamId</td>
<td>StreamId</td>
<td>yes</td>
<td>The stream ID.</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>StreamDescription</td>
<td>no</td>
<td>The description of the stream.</td>
</tr>
<tr>
<td>files</td>
<td>StreamFiles</td>
<td>no</td>
<td>The files associated with the stream.</td>
</tr>
<tr>
<td>roleArn</td>
<td>RoleArn</td>
<td>no</td>
<td>An IAM role that allows the IoT service principal assumes to access your S3 files.</td>
</tr>
</tbody>
</table>

**Response syntax:**
Content-type: application/json
{
  "streamId": "string",
  "streamArn": "string",
  "description": "string",
  "streamVersion": "integer"
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streamId</td>
<td>StreamId</td>
<td>no</td>
<td>The stream ID.</td>
</tr>
<tr>
<td>streamArn</td>
<td>StreamArn</td>
<td>no</td>
<td>The stream ARN.</td>
</tr>
<tr>
<td>description</td>
<td>StreamDescription</td>
<td>no</td>
<td>A description of the stream.</td>
</tr>
<tr>
<td>streamVersion</td>
<td>StreamVersion</td>
<td>no</td>
<td>The stream version.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException
   The contents of the request were invalid. For example, this code is returned when an
   UpdateJobExecution request contains invalid status details. The message contains details about the
   error.
   HTTP response code: 400

ResourceNotFoundException
   The specified resource does not exist.
   HTTP response code: 404

ThrottlingException
   The rate exceeds the limit.
   HTTP response code: 429

UnauthorizedException
   You are not authorized to perform this operation.
   HTTP response code: 401

ServiceUnavailableException
   The service is temporarily unavailable.
   HTTP response code: 503

InternalFailureException
   An unexpected error has occurred.
   HTTP response code: 500

cli

Synopsis:
aws iot update-stream \
--stream-id <value> \ 
[--description <value>] \ 
[--files <value>] \ 
[--role-arn <value>] \ 
[--cli-input-json <value>] \ 
[--generate-cli-skeleton]

cli-input-json format:

```
{
   "streamId": "string",
   "description": "string",
   "files": [
      {
         "fileId": "integer",
         "s3Location": {
            "bucket": "string",
            "key": "string",
            "version": "string"
         }
      }
   ],
   "roleArn": "string"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streamId</td>
<td>string</td>
<td>The stream ID.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td>pattern: [a-zA-Z0-9-_]+</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>The description of the stream.</td>
</tr>
<tr>
<td></td>
<td>length- max:2028</td>
<td>pattern: ^\p{C}+</td>
</tr>
<tr>
<td>files</td>
<td>list</td>
<td>The files associated with the stream.</td>
</tr>
<tr>
<td>fileld</td>
<td>integer</td>
<td>The file ID.</td>
</tr>
<tr>
<td></td>
<td>range- max:255 min:0</td>
<td></td>
</tr>
<tr>
<td>s3Location</td>
<td>S3Location</td>
<td>The location of the file in S3.</td>
</tr>
<tr>
<td>bucket</td>
<td>string</td>
<td>The S3 bucket that contains the file to stream.</td>
</tr>
<tr>
<td></td>
<td>length- min:1</td>
<td></td>
</tr>
<tr>
<td>key</td>
<td>string</td>
<td>The name of the file within the S3 bucket to stream.</td>
</tr>
<tr>
<td></td>
<td>length- min:1</td>
<td></td>
</tr>
<tr>
<td>version</td>
<td>string</td>
<td>The file version.</td>
</tr>
</tbody>
</table>

1108
UpdateStream

### Name | Type | Description
--- | --- | ---
roleArn | string | An IAM role that allows the IoT service principal assumes to access your S3 files.

**Output:**

```json
{
  "streamId": "string",
  "streamArn": "string",
  "description": "string",
  "streamVersion": "integer"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>streamId</td>
<td>string</td>
<td>The stream ID.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9-]+</td>
<td></td>
</tr>
<tr>
<td>streamArn</td>
<td>string</td>
<td>The stream ARN.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>A description of the stream.</td>
</tr>
<tr>
<td></td>
<td>length- max:2028 pattern: [^\p{C}]+</td>
<td></td>
</tr>
<tr>
<td>streamVersion</td>
<td>integer</td>
<td>The stream version.</td>
</tr>
<tr>
<td></td>
<td>range- max:65535 min:0</td>
<td></td>
</tr>
</tbody>
</table>

**Errors:**

- **InvalidRequestException**
  The contents of the request were invalid. For example, this code is returned when an `UpdateJobExecution` request contains invalid status details. The message contains details about the error.

- **ResourceNotFoundException**
  The specified resource does not exist.

- **ThrottlingException**
  The rate exceeds the limit.

- **UnauthorizedException**
  You are not authorized to perform this operation.

- **ServiceUnavailableException**
  The service is temporarily unavailable.
InternalFailureException
An unexpected error has occurred.

UpdateThing

Updates the data for a thing.

https

Request syntax:

```
PATCH /things/thingName
Content-type: application/json

{
  "thingTypeName": "string",
  "attributePayload": {
    "attributes": {
      "string": "string"
    },
    "merge": "boolean"
  },
  "expectedVersion": "long",
  "removeThingType": "boolean"
}
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing to update.</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingTypeName</td>
<td>ThingTypeName</td>
<td>no</td>
<td>The name of the thing type.</td>
</tr>
</tbody>
</table>
| attributePayload| AttributePayload    | no   | A list of thing attributes, a JSON string containing name-value pairs. For example:

```
"attributes":{}
  "name1": "value2"
```

This data is used to add new attributes or update existing attributes.
### AWS IoT Developer Guide

#### UpdateThing

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>expectedVersion</td>
<td>OptionalVersion</td>
<td>no</td>
<td>The expected version of the thing record in the registry. If the version of the record in the registry does not match the expected version specified in the request, the UpdateThing request is rejected with a VersionConflictException.</td>
</tr>
<tr>
<td>removeThingType</td>
<td>RemoveThingType</td>
<td>no</td>
<td>Remove a thing type association. If true, the association is removed.</td>
</tr>
</tbody>
</table>

#### Errors:

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

**VersionConflictException**

An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

HTTP response code: 409

**ThrottlingException**

The rate exceeds the limit.

HTTP response code: 429

**UnauthorizedException**

You are not authorized to perform this operation.

HTTP response code: 401

**ServiceUnavailableException**

The service is temporarily unavailable.

HTTP response code: 503

**InternalFailureException**

An unexpected error has occurred.

HTTP response code: 500

**ResourceNotFoundException**

The specified resource does not exist.
HTTP response code: 404

cli

Synopsis:

```
aws iot update-thing \
  --thing-name <value> \ 
  [- --thing-type-name <value>] \ 
  [- --attribute-payload <value>] \ 
  [- --expected-version <value>] \ 
  [- --remove-thing-type | --no-remove-thing-type] \ 
  [- --cli-input-json <value>] \ 
  [- --generate-cli-skeleton] 
```

cli-input-json format:

```
{
  "thingName": "string",
  "thingTypeName": "string",
  "attributePayload": {
    "attributes": {
      "string": "string"
    },
    "merge": "boolean"
  },
  "expectedVersion": "long",
  "removeThingType": "boolean"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing to update.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>thingTypeName</td>
<td>string</td>
<td>The name of the thing type.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9-_]+</td>
<td></td>
</tr>
<tr>
<td>attributePayload</td>
<td>AttributePayload</td>
<td>A list of thing attributes, a JSON string containing name-value pairs. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;attributes&quot;:{&quot;name1&quot;:&quot;value2&quot;}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This data is used to add new attributes or update existing attributes.</td>
</tr>
<tr>
<td>attributes</td>
<td>map</td>
<td>A JSON string containing up to three key-value pair in JSON format. For example:</td>
</tr>
</tbody>
</table>

1112
Name | Type | Description
--- | --- | ---
attributes | string | 

merge | boolean | Specifies whether the list of attributes provided in the AttributePayload is merged with the attributes stored in the registry, instead of overwriting them.

To remove an attribute, call UpdateThing with an empty attribute value.

**Note**
The merge attribute is only valid when calling UpdateThing.

expectedVersion | long | The expected version of the thing record in the registry. If the version of the record in the registry does not match the expected version specified in the request, the UpdateThing request is rejected with a VersionConflictException.

removeThingType | boolean | Remove a thing type association. If true, the association is removed.

Output:
None

Errors:

**InvalidRequestException**
The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

**VersionConflictException**
An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

**ThrottlingException**
The rate exceeds the limit.

**UnauthorizedException**
You are not authorized to perform this operation.

**ServiceUnavailableException**
The service is temporarily unavailable.
InternalFailureException

An unexpected error has occurred.

ResourceNotFoundException

The specified resource does not exist.

UpdateThingGroup

Update a thing group.

https

Request syntax:

```plaintext
PATCH /thing-groups/thingGroupName
Content-type: application/json
{
  "thingGroupProperties": {
    "thingGroupDescription": "string",
    "attributePayload": {
      "attributes": {
        "string": "string"
      },
      "merge": "boolean"
    }
  },
  "expectedVersion": "long"
}
```

URI Request Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>ThingGroupName</td>
<td>yes</td>
<td>The thing group to update.</td>
</tr>
</tbody>
</table>

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupProperties</td>
<td>ThingGroupProperties</td>
<td>yes</td>
<td>The thing group properties.</td>
</tr>
<tr>
<td>expectedVersion</td>
<td>OptionalVersion</td>
<td>no</td>
<td>The expected version of the thing group. If this does not match the version of the thing group being updated, the update will fail.</td>
</tr>
</tbody>
</table>

Response syntax:

```plaintext
Content-type: application/json
```
Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>Version</td>
<td>no</td>
<td>The version of the updated thing group.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

VersionConflictException

An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

HTTP response code: 409

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

cli

Synopsis:

```
aws iot update-thing-group \
  --thing-group-name <value> \
  --thing-group-properties <value> \
  [--expected-version <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "thingGroupName": "string",
  "thingGroupProperties": {
```
UpdateThingGroup

"thingGroupDescription": "string",
"attributePayload": {
    "attributes": {
        "string": "string"
    },
    "merge": "boolean"
},
"expectedVersion": "long"

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingGroupName</td>
<td>string</td>
<td>The thing group to update.</td>
</tr>
<tr>
<td>length- max:128 min:1</td>
<td>pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>thingGroupProperties</td>
<td>ThingGroupProperties</td>
<td>The thing group properties.</td>
</tr>
<tr>
<td>thingGroupDescription</td>
<td>string</td>
<td>The thing group description.</td>
</tr>
<tr>
<td>length- max:2028</td>
<td>pattern: [\p{Graph}]*</td>
<td></td>
</tr>
<tr>
<td>attributePayload</td>
<td>AttributePayload</td>
<td>The thing group attributes in JSON format.</td>
</tr>
<tr>
<td>attributes</td>
<td>map</td>
<td>A JSON string containing up to three key-value pair in JSON format. For example:</td>
</tr>
<tr>
<td>merge</td>
<td>boolean</td>
<td>Specifies whether the list of attributes provided in the AttributePayload is merged with the attributes stored in the registry, instead of overwriting them.</td>
</tr>
<tr>
<td>expectedVersion</td>
<td>long</td>
<td>The expected version of the thing group. If this does not match the version of the thing group being updated, the update will fail.</td>
</tr>
</tbody>
</table>
Output:

```json
{
    "version": "long"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>long</td>
<td>The version of the updated thing group.</td>
</tr>
</tbody>
</table>

**Errors:**

**InvalidRequestException**

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

**VersionConflictException**

An exception thrown when the version of a thing passed to a command is different than the version specified with the --version parameter.

**ThrottlingException**

The rate exceeds the limit.

**InternalFailureException**

An unexpected error has occurred.

**ResourceNotFoundException**

The specified resource does not exist.

---

**UpdateThingGroupsForThing**

Updates the groups to which the thing belongs.

https

**Request syntax:**

```json
PUT /thing-groups/updateThingGroupsForThing
Content-type: application/json

{
    "thingName": "string",
    "thingGroupsToAdd": [
        "string"
    ],
    "thingGroupsToRemove": [
        "string"
    ]
}
```
**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>no</td>
<td>The thing whose group memberships will be updated.</td>
</tr>
<tr>
<td>thingGroupsToAdd</td>
<td>ThingGroupList</td>
<td>no</td>
<td>The groups to which the thing will be added.</td>
</tr>
<tr>
<td>thingGroupsToRemove</td>
<td>ThingGroupList</td>
<td>no</td>
<td>The groups from which the thing will be removed.</td>
</tr>
</tbody>
</table>

**Errors:**

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

ResourceNotFoundException

The specified resource does not exist.

HTTP response code: 404

**cli**

**Synopsis:**

```
aws iot update-thing-groups-for-thing \
  [--thing-name <value>] \
  [--thing-groups-to-add <value>] \
  [--thing-groups-to-remove <value>] \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

**cli-input-json format:**

```json
{
  "thingName": "string",
  "thingGroupsToAdd": ["string"
```
UpdateThingShadow

Updates the shadow for the specified thing.

For more information, see UpdateThingShadow in the AWS IoT Developer Guide.

https

Request syntax:

```
POST /things/thingName/shadow
Content-type: application/json
```
UpdateThingShadow

```json
{
  "payload": "blob"
}
```

**URI Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>ThingName</td>
<td>yes</td>
<td>The name of the thing.</td>
</tr>
</tbody>
</table>

**Request Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>payload</td>
<td>JsonDocument</td>
<td>yes</td>
<td>The state information, in JSON format.</td>
</tr>
</tbody>
</table>

**Response syntax:**

```
Content-type: application/json
{
  "payload": "blob"
}
```

**Response Body Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>payload</td>
<td>JsonDocument</td>
<td>no</td>
<td>The state information, in JSON format.</td>
</tr>
</tbody>
</table>

**Errors:**

- **ConflictException**
  - The specified version does not match the version of the document.
  - HTTP response code: 409

- **RequestEntityTooLargeException**
  - The payload exceeds the maximum size allowed.
  - HTTP response code: 413

- **InvalidRequestException**
  - The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
  - HTTP response code: 400

- **ThrottlingException**
  - The rate exceeds the limit.
HTTP response code: 429
UnauthorizedException
You are not authorized to perform this operation.

HTTP response code: 401
ServiceUnavailableException
The service is temporarily unavailable.

HTTP response code: 503
InternalFailureException
An unexpected error has occurred.

HTTP response code: 500
MethodNotAllowedException
The specified combination of HTTP verb and URI is not supported.

HTTP response code: 405
UnsupportedDocumentEncodingException
The encoding is not supported.

HTTP response code: 415

cli

Synopsis:

```
aws iot-data update-thing-shadow \
  --thing-name <value> \
  --payload <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```
{
  "thingName": "string",
  "payload": "blob"
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>thingName</td>
<td>string</td>
<td>The name of the thing.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pattern: [a-zA-Z0-9_:-]+</td>
<td></td>
</tr>
<tr>
<td>payload</td>
<td>blob</td>
<td>The state information, in JSON format.</td>
</tr>
</tbody>
</table>
Output:

```json
{
   "payload": "blob"
}
```

**cli output fields:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>payload</td>
<td>blob</td>
<td>The state information, in JSON format.</td>
</tr>
</tbody>
</table>

**Errors:**

- **ConflictException**
  The specified version does not match the version of the document.
- **RequestEntityTooLargeException**
  The payload exceeds the maximum size allowed.
- **InvalidRequestException**
  The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.
- **ThrottlingException**
  The rate exceeds the limit.
- **UnauthorizedException**
  You are not authorized to perform this operation.
- **ServiceUnavailableException**
  The service is temporarily unavailable.
- **InternalFailureException**
  An unexpected error has occurred.
- **MethodNotAllowedException**
  The specified combination of HTTP verb and URI is not supported.
- **UnsupportedDocumentEncodingException**
  The encoding is not supported.

---

**ValidateSecurityProfileBehaviors**

Validates a Device Defender security profile behaviors specification.

**https**

**Request syntax:**

---

1122
POST /security-profile-behaviors/validate
Content-type: application/json

{
  "behaviors": [
    {
      "name": "string",
      "metric": "string",
      "criteria": {
        "comparisonOperator": "string",
        "value": {
          "count": "long",
          "cidrs": [
            "string"
          ],
          "ports": [
            "integer"
          ],
          "durationSeconds": "integer"
        }
      }
    }
  ]
}

Request Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>behaviors</td>
<td>Behaviors</td>
<td>yes</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
</tbody>
</table>

Response syntax:

Content-type: application/json

{
  "valid": "boolean",
  "validationErrors": [
    {
      "errorMessage": "string"
    }
  ]
}

Response Body Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Req?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>valid</td>
<td>Valid</td>
<td>no</td>
<td>True if the behaviors were valid.</td>
</tr>
<tr>
<td>validationErrors</td>
<td>ValidationErrors</td>
<td>no</td>
<td>The list of any errors found in the behaviors.</td>
</tr>
</tbody>
</table>

Errors:
InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

HTTP response code: 400

ThrottlingException

The rate exceeds the limit.

HTTP response code: 429

InternalFailureException

An unexpected error has occurred.

HTTP response code: 500

cli

Synopsis:

```
aws iot validate-security-profile-behaviors \
  --behaviors <value> \
  [--cli-input-json <value>] \
  [--generate-cli-skeleton]
```

cli-input-json format:

```json
{
  "behaviors": [
    {
      "name": "string",
      "metric": "string",
      "criteria": {
        "comparisonOperator": "string",
        "value": {
          "count": "long",
          "cidrs": [
            "string"
          ],
          "ports": [
            "integer"
          ],
        },
        "durationSeconds": "integer"
      }
    }
  ]
}
```

cli-input-json fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>behaviors</td>
<td>list</td>
<td>Specifies the behaviors that, when violated by a device (thing), cause an alert.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>The name you have given to the behavior.</td>
</tr>
<tr>
<td></td>
<td>length- max:128 min:1 pattern: [a-zA-Z0-9:_-]+</td>
<td></td>
</tr>
<tr>
<td>metric</td>
<td>string</td>
<td>What is measured by the behavior.</td>
</tr>
<tr>
<td>criteria</td>
<td>BehaviorCriteria</td>
<td>The criteria that determine if a device is behaving normally in regard to the metric.</td>
</tr>
<tr>
<td>comparisonOperator</td>
<td>string</td>
<td>The operator that relates the thing measured (metric) to the criteria (value).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enum: less-than</td>
</tr>
<tr>
<td>value</td>
<td>MetricValue</td>
<td>The value to be compared with the metric.</td>
</tr>
<tr>
<td>count</td>
<td>long</td>
<td>If the comparisonOperator calls for a numeric value, use this to specify that numeric value to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>range- min:0</td>
<td></td>
</tr>
<tr>
<td>cidrs</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of CIDRs, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>member: Cidr</td>
<td></td>
</tr>
<tr>
<td>ports</td>
<td>list</td>
<td>If the comparisonOperator calls for a set of ports, use this to specify that set to be compared with the metric.</td>
</tr>
<tr>
<td></td>
<td>member: Port</td>
<td></td>
</tr>
<tr>
<td>durationSeconds</td>
<td>integer</td>
<td>Use this to specify the period of time over which the behavior is evaluated, for those criteria which have a time dimension (for example, NUM_MESSAGES_SENT).</td>
</tr>
</tbody>
</table>

Output:

```json
{
    "valid": "boolean",
    "validationErrors": [
    {
        "errorMessage": "string"
    }
}
```
cli output fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>valid</td>
<td>boolean</td>
<td>True if the behaviors were valid.</td>
</tr>
<tr>
<td>validationErrors</td>
<td>list</td>
<td>The list of any errors found in the behaviors.</td>
</tr>
<tr>
<td>member: ValidationError</td>
<td></td>
<td></td>
</tr>
<tr>
<td>errorMessage</td>
<td>string length- max:2048</td>
<td>The description of an error found in the behaviors.</td>
</tr>
</tbody>
</table>

Errors:

InvalidRequestException

The contents of the request were invalid. For example, this code is returned when an UpdateJobExecution request contains invalid status details. The message contains details about the error.

ThrottlingException

The rate exceeds the limit.

InternalFailureException

An unexpected error has occurred.